CONFIGURACIÓN DE UN BACK-UP ACTIVO – ACTIVO CON SELECCIÓN DE TRÁFICO EN UN CANAL DEDICADO DE DATOS PARA LA EMPRESA ENERCOM S.A.S

ANDRÉS FELIPE ZORRILLA MOLINA

Proyecto de Grado

Tutor

Alvaro Escobar Escobar

Director Especialización en Telecomunicaciones

UNIVERSIDAD PILOTO DE COLOMBIA

FACULTAD DE INGENIERIA

ESPECIALIZACIÓN EN TELECOMUNICACIONES

BOGOTÁ

2016

CONTENIDO

pág.

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

ACL[1]: lista de control de acceso (del inglés, Access Control List) controlar el flujo de tráfico de los paquetes en equipos de red que funcionan en la capa 3 del modelo OSI. Su principal objetivo es permitir o denegando el tráfico de los paquetes de acuerdo a alguna condición.

ANCHO DE BANDA[2]: en informática y telecomunicaciones, define la velocidad a la que puede transmitirse la información binaria en un tiempo definido entre dos dispositivos digitales. Es la velocidad de transmisión de datos.

BACK-UP[3]: copia de respaldo, en telecomunicaciones este término es utilizado para los canales de comunicación que sirven de respaldo o contingencia de un canal principal para evitar fallas en la comunicación.

ICMP[4]: protocolo de mensajes de control de Internet (en inglés, Internet Control Message Protocol) es un protocolo utilizado por los equipos de red para enviar mensajes de estado de error, este protocolo es utilizado por algunas herramientas de diagnóstico como ping y traceroute.

---

[1] Cisco System. Access control list: overview and guidelines [en línea]. Version 12.2. San José (California). Cisco System. [Citado en 2016-02-03]. Disponible en: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfacls.html#wp1000893

[2] BATEMAN, Andy. Comunicaciones digitales diseño para el mundo real. España. Marcambo S.A. 2003. 223p

[3] FREEDMAN, Alan. Glosario de computación. México. McGraw-Hill. 1984. 396 p.

[4] ROMERO TERNERO, María del Carmen, et ali. Redes locales. ed. 2ª. España. Parainfo S.A. 2014. 294 p.

IOS[5]: (en inglés, Internetwork Operating System) es un software de infraestructura de red que proporciona las funcionalidades para los servicios de red, este software es utilizado en los equipos de red de la empresa Cisco System.

ISP: proveedor de servicio de Internet (en inglés, Internet Service Provider) es la empresa que a través de su infraestructura puede conectar a los clientes a internet.

WIFI-MESH: conjunto de puntos de acceso WiFi organizados en una topología de malla que permite ampliar la cobertura del servicio.

PBR[6]: enrutamiento basado en políticas (en inglés, Policy Based Routing) técnica de enrutamiento que permite redireccionar paquetes dependiendo de las políticas configuradas en el enrutador.

PING: "Usa los mensajes ICMP solicitud de eco y respuesta de eco para determinar si un host es alcanzable y medir el tiempo que tarda en llegar la respuesta a la solicitud de eco desde dicho host"[7].

PMP: punto multipunto, en telecomunicaciones es una tecnología de comunicación microondas que permite conectar múltiples puntos remotos a un solo punto central.

[5] Cisco System. Software de red (IOS y NX-OS) [en línea]. San jose (California). Cisco System. [citado en 2016-02-28]. Disponible en: http://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-software-releases-listing.html

[6] HEWLETT-PACKARD. Policy based routing. Texas. Hewlett-packard [citado en 2015-03-15]. Disponible en: https://www.google.com/patents/US20140029619

[7] ROMERO TERNERO, María del Carmen, et ali. Redes locales. ed. 2ª. España. Parainfo S.A. 2014. 294 p

PTP: punto a punto (en inglés, Point To Point) en telecomunicaciones es una tecnología de comunicación microondas que permite conectar solo dos puntos.

ROUTER: también conocido como enrutador, es un dispositivo que encamina los paquetes de datos para conectar una o varias redes.

RUTA ESTÁTICA: comando que le permite a un enrutador determinar el camino a donde se debe enviar un paquete de datos.

TABLA DE ENRUTAMIENTO: Es la información que consulta los enrutadores y equipos de red para determinar hacia donde debe ser enviado los paquetes entrantes.

TRACK: herramienta utilizada en los enrutadores para seguir o rastrear el comportamiento de un objeto en particular.

INTRODUCCIÓN

Desde 1878 cuando se iniciaron las pruebas experimentales de comunicación telefónica en Colombia y con los continuos avances informáticos y de comunicaciones que permitieron que cada vez más empresas lograran comunicarse con sus propias sucursales se creó una fuerte dependencia a estos canales de comunicación, convirtiéndose en muchos casos en piezas fundamentales para la continuidad de los negocios, tratando de prevenir las fallas de estos canales se empezaron a utilizar los canales de respaldo o back-up logrando tener una alta disponibilidad de la comunicación.

Mediante este proyecto de investigación se mostrará como configurar los canales de comunicación de respaldo o back-up de los clientes de la empresa Enercom para darles un nuevo enfoque ya que normalmente estos canales permanecen pasivos dentro de la red aguardando el momento en que el canal principal falle para entrar en funcionamiento, se pretende lograr que tanto el canal principal como el canal de back-up estén en todo momento operativos pasando tráfico y que a su vez uno sea el respaldo del otro cuando se presenten fallas, logrando una alta disponibilidad y maximizando los recursos de comunicación aportando una mejor experiencia para el usuario final debido a un aumento de ancho de banda, además, brindarle al cliente la posibilidad de seleccionar por cuál de los canales enviará su tráfico más relevante.

1. JUSTIFICACIÓN

Con el trascurrir del tiempo y con los avances tecnológicos, informáticos y de telecomunicaciones se ha generado una dependencia cada vez más fuerte a la tecnología y las comunicaciones, es por eso que en la actualidad toda empresa por pequeña que sea utiliza recursos tecnológicos y de comunicaciones como internet, canales dedicados de datos, voz sobre IP, mercadeo en la web, transacciones electrónicas, etc. Para poder competir en el mercado y lograr mejores ganancias.

Enercom S.A. es una empresa de comunicaciones que tiene clientes en el sector de hidrocarburos los cuales exigen canales de comunicación entre sus sedes principales en Bogotá y los campos de producción y perforación con alta disponibilidad y una redundancia automática en caso de fallas, en el informe anual que se realiza a los clientes uno de ellos observo que para varias de las sedes de producción tenían canales dedicas de datos con un back-up de iguales características al principal pero que prácticamente no se utilizaba ya que en el 2014 se tuvo una buena disponibilidad de los enlaces principales, al observar esta situación el cliente concluyó que para el 2015 era necesario que ambos canales estuvieran activos, que se pudiera elegir por cuál de ellos enviar el tráfico más importante dependiendo del desempeño de los canales y que uno fuera back-up del otro por si llegaban a fallar y así logra optimizar los recursos que invierten en comunicaciones para dar un mejor servicio a los usuarios finales.

Con este trabajo de investigación se pretende conocer e implementar las técnicas y protocolos necesarios para lograr que en un canal de comunicaciones con back-up ambos puedan estar activos, es decir, que los dos canales tengan tráfico en todo momento pero que se pueda seleccionar que paquetes van a ir por cada canal dependiendo de los criterios de selección del cliente, además un canal debe ser back-up del otro evitando la indisponibilidad en caso de fallas. De esta manera se lograría aumentar el ancho de banda disponible para los clientes con canales de back-up cuando los dos canales este operativos, esto da como resultado que los usuarios finales tengan un mejor desempeño de sus aplicativos informáticos, navegación en internet y

comunicaciones en general. Enercom S.A. logrará satisfacer las exigencias y necesidades de los clientes de la empresa, además el resultado de esta investigación se convertirá en un nuevo servicio o valor agregado en el portafolio de servicios de la empresa logrando diferenciarse de la competencia.

2. PLANTEAMIENTO DEL PROBLEMA

¿Cómo configurar en un canal de comunicaciones dedicado un back-up activo-activo con selección de tráfico para la empresa Enercom S.A.?

3. OBJETIVOS

3.1 GENERAL

Implementar una configuración en un canal dedicado de datos que permita tener un back-up activo de manera constante con la posibilidad de seleccionar el tráfico que se envía por ambos canales sin perder el funcionamiento normal de un back-up, para los clientes de la empresa Enercom S.A.

3.2 ESPECÍFICOS

- Definir la topología de la red.
- Definir el criterio de selección para el tráfico de la red que permita decidir a los equipos de enrutamiento por donde enviar los paquetes.
- Configurar en los equipos de red protocolos o técnicas que permitan seleccionar el tráfico que será enviado por cada ruta o canal.
- Configurar un protocolo o técnica de enrutamiento que le permita al router decidir cuál es el siguiente salto para los paquetes dependiendo de los criterios de selección de tráfico.
- Realizar pruebas que permitan verificar que los paquetes toman la ruta adecuada según los criterios de selección.

4. MARCO TEÓRICO

4.1 ERUTAMIENTO IP

Los routers consultan su tabla de enrutamiento para determinar hacia donde envían los paquetes recepcionados, el aprendizaje y determinación de estas rutas se hace de forma dinámica a través de protocolos que realizan cálculos para determinar las rutas hacia las redes de destino o estática ejecutando comandos manualmente.

El enrutamiento estático es un método que proporciona un control absoluto sobre las rutas que tendrá la tabla de enrutamiento, es configurado manualmente por el administrador de la red y no sufre cambios en comparación con los protocolos de enrutamiento dinámicos los cuales realizan cálculos automáticos constantes que pueden alterar dinámicamente las tablas de enrutamiento de los routers. El enrutamiento estático es más apropiado cuando una topología de red es pequeña, cuando los enrutadores tienen limitaciones de su rendimiento en cuanto al procesamiento y memoria y cuando se desea tener control total del enrutamiento[8].

4.2 ACL (Access Control List)

Las listas de control de acceso es un método utilizado para filtrar el tráfico que pasa por los routers, se puede permitir o negar los paquetes dependiendo de los criterios que se configuran en las sentencias secuenciales de los ACL, cuando los paquetes ingresan a un router y la interfaz llama una ACL el paquete se evalúa con los criterios del ACL y si estos coinciden se niega o permite que el paquete continúe, esta evaluación es secuencial y si se encuentra una coincidencia el resto de la sentencias del ACL no se comparan[9].

[8] ARIGANELLO, Ernesto. Enrutamiento IP. En. Redes Cisco: Guía de Estudio para la Certificación CCNA 640-802. México: Alfaomega, 2009. P. 57 -59.

[9] Cisco System. Access control list: overview and guidelines [en línea]. Version 12.2. San José (California). Cisco System. [Citado en 2015-03-15]. Disponible en: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfacls.html#wp1000893

También tiene usos diferentes como la de distinguir el trafico interesante o relevante para ciertos propósitos como el QoS (Quality of Service) y voz IP en donde la ACL se encarga de distinguir los paquetes de voz que luego se les dará un tratamiento especial dependiendo de la configuración de QoS. Existen 5 tipos de ACLs los cuales tienen distintos usos:

ACL estándar**:** en este tipo de ACL solo se filtra el tráfico comparando la dirección IP origen de paquete con la dirección configurada en la ACL, este es el formato de la sintaxis de los comandos de una ACL estándar.

access-list access-list-number {permit|deny} {host|source source-wildcard|any}

En todas las ACLs existe una negación de tráfico implícita en donde si no existe una coincidencia con las entradas de la ACL el tráfico es rechazado.

ACL extendida: este tipo de ACL filtra el tráfico comparando las direcciones IP origen y destino del paquete con las direcciones configuradas en la ACL, este es el formato de la sintaxis.

IP: Access-list access-list-number [dynamic dynamic-name [timeoutminutes]] {deny | permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log | log-input] [time-range time-range-name]

ICMP: Access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit} icmp source source-wildcard destination destination-wildcard [icmp-type | [[icmp-type icmp-code] | [icmp-message]] [precedence precedence] [tos tos] [log | log-input] [time-range time-range-name]

TCP: Access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit} tcp source source-wildcard [operator [port]] destination destination-wildcard [operator [port]] [established] [precedence precedence] [tos tos] [log | log-input] [time-range time-range-name]

UDP: Access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit} udp source source-wildcard [operator [port]] destination destination-wildcard [operator [port]] [precedence precedence] [tos tos] [log | log-input] [time-range time-range-name]

ACL nombradas: permite que las ACL estándar y ampliadas reciban un nombre en vez de un número, además se puede hacer la modificación de las entradas de la ACL sin necesidad de borrar toda la lista, este es el formato de la sintaxis.

permit|deny tcp source source-wildcard [operator [port]] destination destination-wildcard [operator [port]] [established] [precedence precedence] [tos tos] [log] [time-range time-range-name]

ACL reflexiva: filtra los paquetes IP según los datos de sesión de capa superior, se utilizan para permitir el tráfico saliente y limitar el tráfico entrante como respuesta a una sesión que se origina al dentro del router, este es el formato de la sintaxis.

interface ip access-group {number|name} {in|out}

ip access-list extended name permit protocol any any reflect name [timeoutseconds]

ip access-list extended name

evaluate name

ACL Basadas en Tiempo: Permite que la ACL se ejecute en un tiempo definido por el administrador de la red, se crea un intervalo de tiempo que define momentos específicos del día y la semana, el intervalo temporal depende del reloj del sistema del router. Este es el formato de la sintaxis.

!--- Define un intervalo de tiempo con nombre.

time-range time-range-name

!--- Define los momentos periódicos.

periodic days-of-the-week hh:mm to [days-of-the-week] hh:mm

!--- O bien, define los tiempos absolutos.

absolute [start time date] [end time date]

!--- El intervalo de tiempo utilizado en la ACL real.

ip access-list name|number time-rangename_of_time-range[10]

Para cumplir con los objetivos de esta investigación se utilizaran las ACLs para identificar el tráfico relevante con criterio particular definidos por el cliente que luego se les dará un enrutamiento específico.

[10] Cisco System. Configuración de listas de acceso IP [en línea]. San José (California). Cisco System. [citado en 2015-03-15]. Disponible en: http://www.cisco.com/cisco/web/support/LA/7/75/75923_confaccesslists.pdf

4.3 ROUTE-MAPS

Los route-map funcionan de manera similar a los ACL y es una herramienta que evalúa sentencias secuenciales para encontrar coincidencia y determinar acciones como permitir o denegar rutas y cambiar la métrica de una ruta, son la base de las políticas basadas en enrutamiento y permiten tomar decisiones complejas sobre el enrutamiento de paquetes.

Una sentencia de route-map puede tener una o más coincidencias que se evalúan con los operadores lógicos OR y AND, contienen una o más sentencias **set** que definen las acciones que se toman para los paquetes, esto hace que se puedan hacer muchas más cosas que con las **ACLs.** La siguiente es la sintaxis de los route-maps.

Route-map *map-tag [{*permit |deny} *sequence-number*][11]

4.4 PBR (Policy Based Routing)

Enrutamiento basado en políticas (PBR) se puede utilizar para tomar decisiones de enrutamiento basado en políticas establecidas por el administrador de red. Típicamente, un router recibe un paquete de datos y decide enviar el paquete de datos teniendo en cuenta la dirección de destino en el paquete de datos. En cambio PBR puede dirigir el paquete de datos para ser transmitido sobre la base de la dirección de origen o destino. PBR también puede dirigir el paquete de datos a ser enviada sobre la base de otros criterios, tales como el tamaño del paquete de datos u otra información disponible en una cabecera de paquete de datos[12].

[11] ARIGANELLO, Ernesto y BARRIENTOS SEVILLA, Enrique. Implementaciones con cisco IOS. En. Redes Cisco CCNP a fondo Guía de estudios para profesionales. México: Alfaomega, 2010. P. 188-191.

[12] HEWLETT-PACKARD. Policy based routing. Texas. Hewlett-packard. [citado en 2015-03-15]. Disponible en: https://www.google.com/patents/US20140029619

El enrutamiento basado en políticas es un mecanismo flexible que permite al administrador de la red anticiparse a las rutas establecidas en la tabla de enrutamiento implementando un reenvió de paquetes dependiendo de sus políticas basadas en ACLs.

4.5 IP SLA (Service level Agreement)

Los acuerdos de nivel de servicio IP es una tecnología que se utiliza para supervisar activamente el tráfico de la red y medir su rendimiento, con IP SLA es posible supervisar y medir los parámetros críticos que ayudan al administrador a conocer el rendimiento y disponibilidad de la red, el resultado de este monitoreo es la posibilidad de anticiparse a los problemas de bajo rendimiento que pueden afectar servicios muy sensibles como la voz sobre IP, fallas por saturación y caídas del servicio.

Se pueden monitorear diversos parámetros de una red con IP SLA, el resultado puede ser transmitido a través de SNMP y utilizados por las aplicaciones de monitoreo de desempeño como Cisco Works, PRTG, Orion, Nagios, etc. IP SLA obtiene parámetros de rendimiento como:

- Delay
- Jitter
- Perdida de paquetes
- Latencia
- Rutas[13]

[13] Cisco System. Configuring IP SLA [en línea]. Versión 12.4. San José (California). Cisco System. [citado en 2015-03-15]. Disponible en: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/44sg/configuration/guide/Wrapper-44SG/swipsla.html

5. CONTEXTUALIZACIÓN EMPRESARIAL

5.1 HISTORIA DE LA EMPRESA

Enercom S.A. nace como una empresa familiar en el año 1988, creada por el Ingeniero Hermes Puentes Camero, luego de trabajar varios años en Caracol decide independizarse y crear la empresa. Enercom inicio ofreciendo servicio de radio de dos vías para la empresa Perenco perteneciente al sector de hidrocarburos en la zona del Casanare. Enercom observa una oportunidad de expandirse al determinar que en estas zonas se tenían varias necesidades de comunicación como lo era la telemétrica de los variadores (equipos de producción en el área petrolera que controlan la extracción de petróleo), servicios de internet, voz sobre IP, servicios de comunicaciones que se puedan migrar fácilmente.

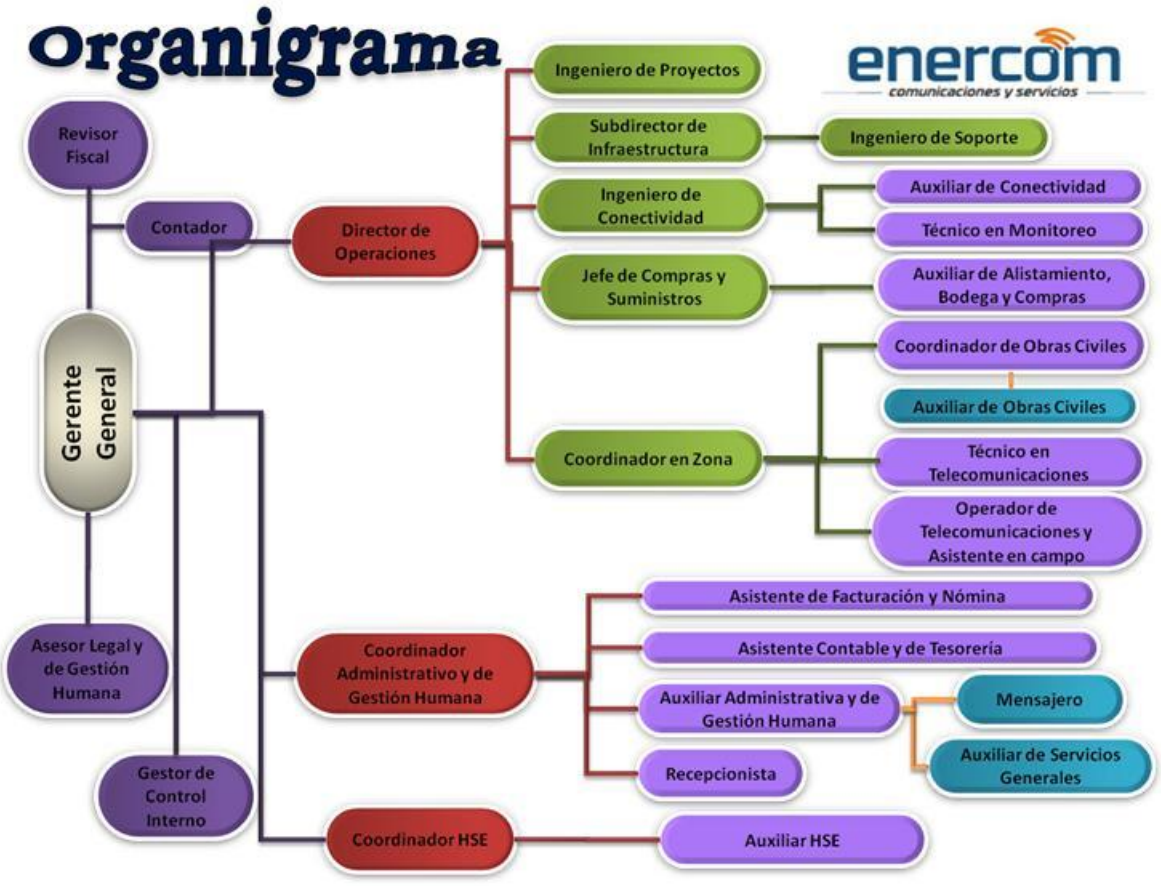
Enercom inicia su crecimiento instalando comunicaciones de corto alcance para los pozos con los cuales se llevaba comunicación hasta el punto principal de recolección de la información, luego se ofrecieron servicios de comunicación satelital que permiten una instalación en cualquier parte de una manera rápida llevando internet e interconectando los pozos de perforación con las sedes principal en Bogotá. Posteriormente se inicia la construcción de torres para comunicación y a crear redes utilizando radios microondas para alcanzar las sedes de producción y perforación permitiendo que la comunicación tuviera mejores tiempos de respuesta y a menor costo que la tecnología satelital.

Varios años después la empresa logra contratos con otras empresas del sector de hidrocarburos que le permite crecer en infraestructura y aumentando su planta de personal para atender varias zonas del país como lo son Caquetá, Cundinamarca, Putumayo y Sucre, brindando varios servicios de comunicación.

5.2 ESTRUCTURA DE LA EMPRESA

Actualmente la empresa cuenta con setenta empleados y presencia permanente en los departamentos de Casanare, Sucre, Caquetá y Cundinamarca. En la figura 1 se muestra la estructura organizacional de la empresa.

Figura 1. Organigrama

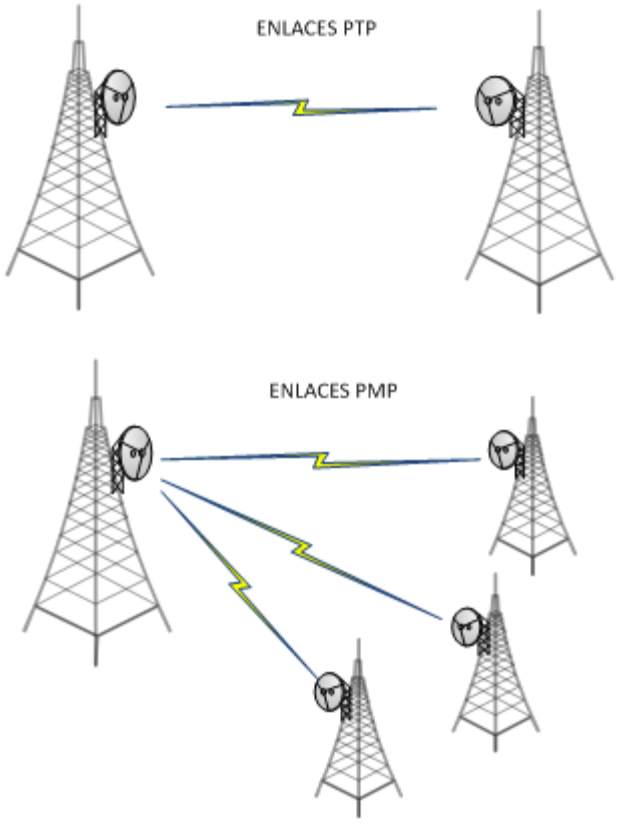


Fuente. Enercom S.A

5.3 PRODUCTOS Y SERVICIOS

- Servicio de enlaces microondas PTP (Point To Point) y PMP (Point To Multipoint): El servicio PTP comunica dos puntos, por lo general se utiliza para enlaces principales. El enlace PMP comunica múltiples puntos con un enlace principal, es utilizado dentro de las locaciones para comunicar varios pozos u oficinas. En la figura 2 se muestra una ilustración de este tipo de conexiones.

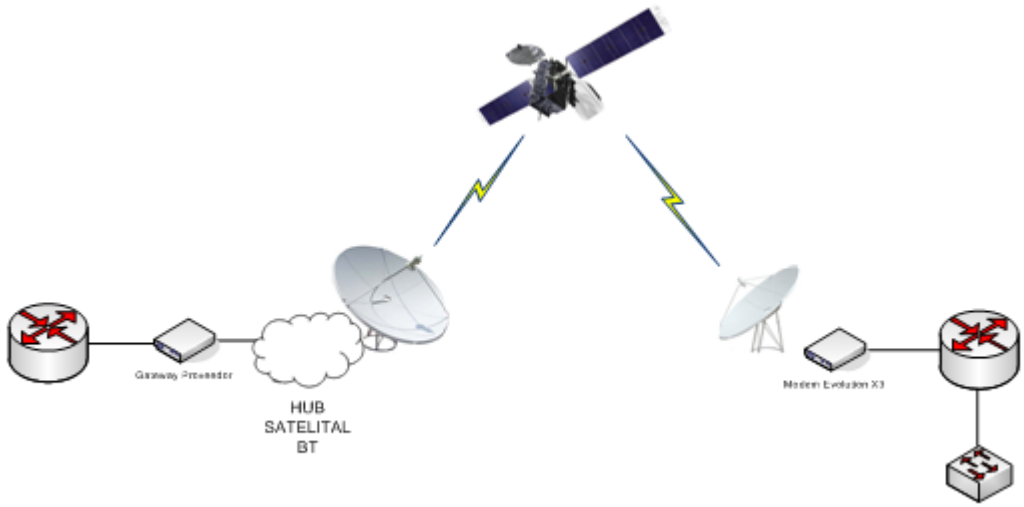
Figura 2. Enlaces PTP y PMP



Fuente. El autor

- Servicio de enlace Satelital: proporciona comunicación de radio satelital en puntos muy aparatados donde las redes convencionales no tienen cobertura. Este tipo de servicio se muestra a continuación en la figura 3.

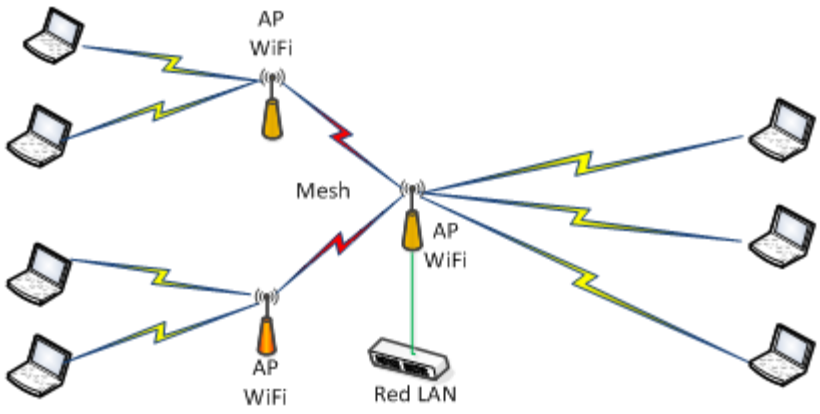
Figura 3. Enlace satelital



Fuente. El autor

• Servicio WiFi – Mesh: En la figura 4 se muestra el servicio de comunicación WiFi con la posibilidad de Mesh (Malla) para cubrir una zona amplia generalmente utilizada en los campos de producción.

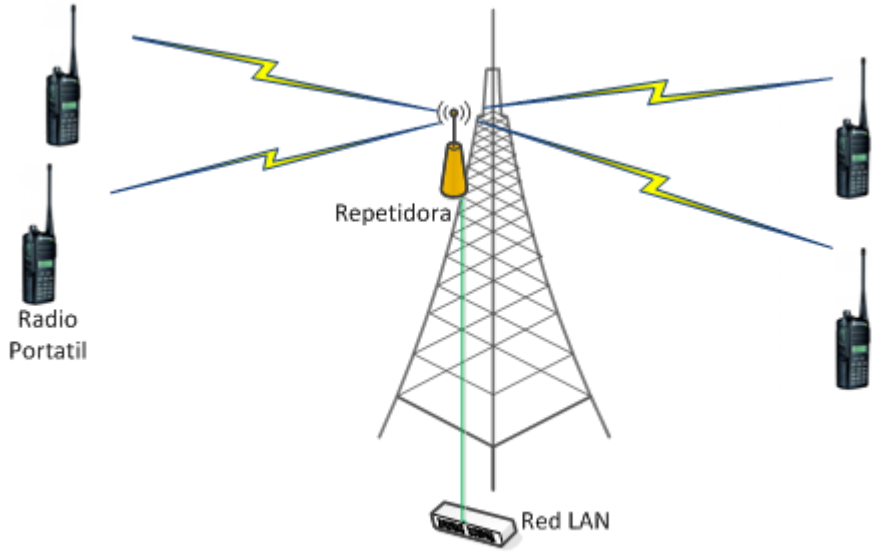
Figura 4. Servicio mesh



Fuente. El autor

- Servicio de comunicación de 2 vías: Este servicio proporciona comunicación de voz con radios portátiles de mano en una zona específica, como se muestra en la figura 5.

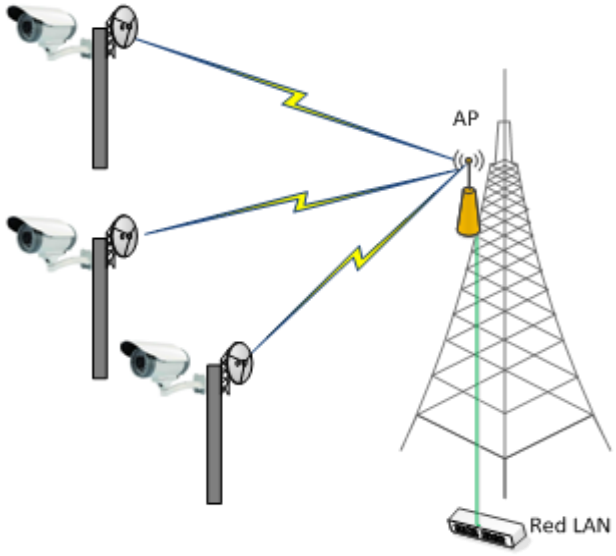
Figura 5. Servicio de radio de 2 vías



Fuente. El autor

- Servicio de monitoreo por video: Servicio de video vigilancia normalmente instalado en campos de producción y pozos de perforación, por lo general se configura con una conexión PMP, ver figura 6.

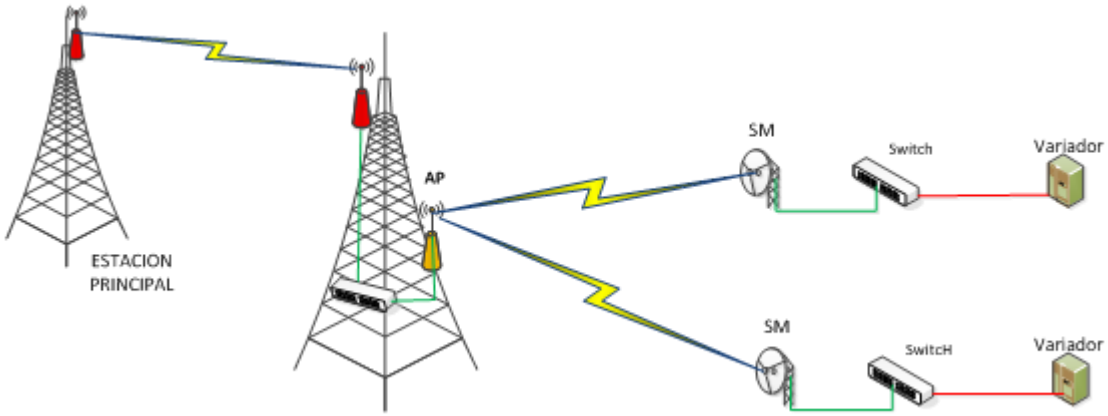
Figura 6. Servicio de video vigilancia



Fuente. El autor

- Servicio de Telemetría: Comunicación desde el pozo de producción hasta el punto principal de recolección de información y control, permite obtener en tiempo real las variables de medición de la extracción del petróleo. En la figura 7 se ilustra la conexión de telemetría la cual puede utilizar radios PMP y PTP.

Figura 7. Servicio de telemetría



Fuente. El autor

5.4 CLIENTES

La totalidad de los clientes de Enercom Pertenecen al sector de hidrocarburos, este tipo de clientes se caracteriza por exigir una respuesta ágil de sus proveedores y una dinámica que les permita adaptarse a las nuevas exigencias y retos que se plantean día a día.

Para los pozos exploratorios este tipo de clientes solicitan la instalación de comunicaciones de manera muy rápida por lo general en menos de 48 horas y en puntos muy apartados y carentes de las condiciones adecuadas para operar, se debe proporcionar conexión con su sede principal en Bogotá y QoS para transportar servicios como VoIP, internet y datos de aplicativos particulares.

Para los campos de producción exigen anchos de banda más grandes, con redundancia que permitan una alta disponibilidad de las comunicaciones asegurado la operatividad de servicios como VoIP, video vigilancia, internet, aplicativos financieros y de producción.

Para cubrir estas necesidades Enercom instala canales de comunicación satelitales, punto a punto y punto multipunto implementando rutas alternas con distintos medios para garantizar la alta disponibilidad y cumplir con los ANS (Acuerdos de Nivel de Servicio) de los contratos.

6. CONSIDERACIÓN DE ALTERNATIVAS

En búsqueda de cumplir con el objetivo general de tener un canal dedicado con un back-up que siempre este activo, es decir, que en todo momento tenga tráfico, en donde el cliente pueda seleccionar que tipo de tráfico pasara por cada uno de sus canales y sin perder el funcionamiento de un canal de respaldo normal, se plantearon dos posibles soluciones las cuales se detallarán a continuación.

6.1 ENRUTAMIENTO ESTÁTICO DETALLADO

En el desarrollo de la solución al problema planteado se consideró esta primera alternativa en donde simplemente se realizaba un enrutamiento estático detallado con múltiples rutas específicas para satisfacer el criterio de selección del cliente, estas rutas a su vez tiene una ruta de respaldo por si llega a fallar el canal o ruta principal.

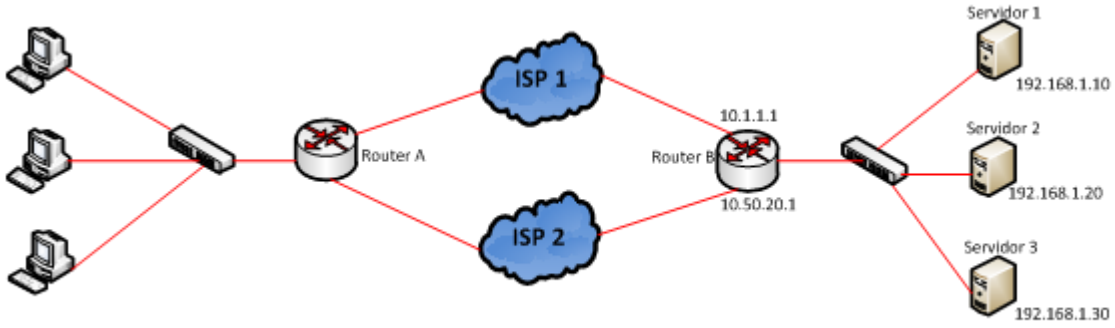
Inicialmente se debe monitorear y verificar la disponibilidad y operatividad de los dos canales, tanto el canal principal como el de back-up, cuando los dos canales están en funcionamiento, es en ese momento donde el enrutamiento detallado y específico decide por cuál de las dos rutas se envían los paquetes para llegar a su destino. Pero si alguno de los dos canales tiene problemas y no está operativo, sea el canal principal o el canal de back-up, la distribución del tráfico dependiendo del criterio de selección del cliente no aplica y simplemente todo el tráfico se envía por la ruta que esté operativa hasta que se recupere la ruta afectada, con esto se logra que los dos canales se brinden respaldo mutuamente.

Para lograr el monitoreo de los 2 canales se utiliza la herramienta IP SLA(Service Level Agreement) del IOS de los routers Cisco y la opción ICMP Echo, esta herramienta permite supervisar y medir los parámetros críticos y la disponibilidad de la red, el router Cisco calcula el tiempo transcurrido

entre el envío de un mensaje de petición de eco ICMP al destino y la respuesta de eco ICMP, esta operación se realiza para los dos canales, principal y back-up, y con esto se determina su operatividad.

Luego se agregan condiciones a las rutas en la tabla de enrutamiento para lograr una distribución del tráfico dependiendo del criterio del cliente. Esto se logra realizando un seguimiento del resultado de los IP SLA con la instrucción Track que permite realizar seguimiento de los estados de los objetos, en este caso del IP SLA, con esta herramienta condicionamos si una ruta entra o no a la tabla de enrutamiento del router y por consiguiente si se utiliza para re-direccionar el tráfico. Tomando como referencia la figura 8 a continuación se muestra un ejemplo de la configuración de un enrutamiento estático detallado:

Figura 8. Topología



Fuente. El autor

Router_A#

ip sla monitor 1

type echo protocol ipIcmpEcho 10.1.1.1 source-interface FastEthernet0/1

```
 timeout 1000
 frequency 5
ip sla monitor schedule 1 life forever start-time now
i
ip sla monitor 2
 type echo protocol ipIcmpEcho 10.50.20.1 source-interface FastEthernet0/0
 timeout 1000
 frequency 5
ip sla monitor schedule 2 life forever start-time now
i
track 1 rtr 1 reachability
i
track 2 rtr 2 reachability
i
ip route 0.0.0.0 0.0.0.0 10.1.1.1 name RUTA_INTERNET_PPAL track 1
ip route 0.0.0.0 0.0.0.0 10.50.20.1 10 name RUTA_INTERNET_BACKUP track 2
ip route 192.168.1.10 255.255.255.255 10.50.20.1 name Ruta1_Servidor1 track 2
ip route 192.168.1.10 255.255.255.255 10.1.1.1 10 name Ruta2_Servidor1 track 1
ip route 192.168.1.20 255.255.255.255 10.50.20.1 name Ruta1_Servidor2 track 2
ip route 192.168.1.20 255.255.255.255 10.1.1.1 10 name Ruta2_Servidor2 track 1
ip route 192.168.1.30 255.255.255.255 10.50.20.1 name Ruta1_Servidor3 track 2
```

ip route 192.168.1.30 255.255.255.255 10.1.1.1 10 name Ruta2_Servidor3 track 1

En este ejemplo siempre existen dos rutas para el mismo destino pero condicionadas por la instrucción track y con una IP de siguiente salto diferente, si ambas rutas están operativas solo una de ellas ingresa a la tabla de enrutamiento ya que la segunda ruta tiene una distancia administrativa más alta.

Si las dos rutas estuvieran operativas el tráfico de internet tomaría la ruta del ISP 1, pero el tráfico hacia los servidores 1,2 y 3 tomaría la ruta del ISP 2.

En caso de que alguno de los ISP falle la tabla de enrutamiento cambiaría y solo tendría ruta por el ISP operativo. Con esto se garantiza de que ambas rutas sean el respaldo una de la otra.

6.2 ENRUTAMIENTO PBR

En esta alternativa se realiza un enrutamiento basado en políticas, esto se conoce como PBR (Policy Based Routing). Para lograr este enrutamiento primero se debe de crear una ACL (Access Control List) con el criterio de selección del cliente para una de las 2 rutas, se puede utilizar cualquier tipo de ACL con el objetivo de lograr capturar el tráfico que el cliente desea que se enrute por una ruta en particular.

Se crea un mapa de ruta (Route-Map) para especificar la distribución de rutas dependiendo de los criterios de su secuencia de comandos, esta herramienta funciona de manera similar a las ACL ya que son un grupo ordenado de sentencias que se evalúan secuencialmente hasta que se encuentra un criterio que coincide. En este rout-map se determina que ruta deben tomar los

paquetes que coinciden con el criterio de selección configurado en la ACL y dependiendo de la evaluación del estado de las rutas que como en el ejemplo anterior se realiza utilizando el IP SLA, y el comando Track para determinar el estado de la rutas.

Se configura una Política (Policy) en la interfaz LAN del router en donde se llama a este route – map, con esto se asegura que todos los paquetes que se originan en la red LAN son evaluados para determinar si coinciden con el criterio de selección del cliente y determinar su ruta para llegar al destino. Ejemplo, tomando como referencia la figura 8.

```
interface FastEthernet0/3
 description CONEXION LAN
 ip address 172.16.10.1 255.255.255.0
ip policy route-map PRINCIPAL
 speed auto
 dúplex auto
!
ip sla monitor 1
 type echo protocol ipIcmpEcho 10.1.1.1 source-interface FastEthernet0/1
 timeout 1000
 frequency 5
ip sla monitor schedule 1 life forever start-time now
i
```

```
ip sla monitor 2
 type echo protocol ipIcmpEcho 10.50.20.1 source-interface FastEthernet0/0
 timeout 1000
 frequency 5
ip sla monitor schedule 2 life forever start-time now
!
track 2 rtr 2 reachability
!
track 2 rtr 2 reachability
!
ip access-list extended SERVIDORES
 permit ip any 192.168.1.10 0.0.0.0
permit ip any 192.168.1.20 0.0.0.0
permit ip any 192.168.1.30 0.0.0.0
!
route-map PRINCIPAL permit 10
 match ip address SERVIDORES
 set ip next-hop verify-availability 10.50.20.1 1 track 2
 set ip next-hop 192.168.95.129
!
ip route 0.0.0.0 0.0.0.0 10.1.1.1 name RUTA_INTERNET_PPAL track 1
```

ip route 0.0.0.0 0.0.0.0 10.50.20.1 10 name RUTA_INTERNET_BACKUP track 2

En este ejemplo el router primero evalúa la política que es invocada en la interfaz LAN y determina el siguiente salto del paquete y posteriormente continúa con su proceso normal de verificar su tabla de enrutamiento para determinar el siguiente salto de los paquetes.

6.3 VENTAJAS Y DESVENTAJAS

En el cuadro 1 se realiza un comparativo de las ventajas y desventajas de las dos alternativas planteadas para cumplir con la configuración de un canal dedicado con un back-up que siempre este activo y en donde se pueda seleccionar el tráfico que se enviará por cada canal.

Cuadro 1. Ventajas y desventajas

Ventajas y desventajas	**Enrutamiento PBR**	**Enrutamiento estático detallado**
Monitoreo de operatividad canal principal	✓	✓
Monitoreo de operatividad canal de back-up	✓	✓
Conmutación de canal principal a back-up y viceversa	✓	✓
Alto consumo de recursos de hardware del router	✓	X
Conocimientos avanzados del administrador de la red para realizar la configuración del router	✓	X
Facilidad para administrar y modificar la configuración del router	✓	X

Cuadro 1. (Continuación)

Ventajas y desventajas	Enrutamiento PBR	Enrutamiento estático detallado
Permite opciones detalladas para seleccionar el tráfico según criterio del cliente	✓	X
Canal principal y back-up activos en todo momento	✓	✓

Fuente. El autor

En el enrutamiento estático detallado se debe configurar una ruta para cada canal dependiendo del criterio del cliente, esto hace que la configuración se torne muy dispendiosa, larga y añade más carga al administrador para mantener y modificar la configuración del router. En esta opción existe una limitante con respecto al criterio de selección del cliente ya que solo se puede lograr la distribución de tráfico determinando la red o IP destino del paquete, por ejemplo: todos los paquetes que tienen como destino el servidor de correo, todos los paquetes que tienen como destino la subred de contabilidad, etc.

En el enrutamiento PBR es necesario que el administrador tenga conocimientos avanzados en la configuración del router, además esta configuración consume recursos adicionales del router ya que antes de realizar su proceso de enrutamiento normal debe ejecutar las instrucciones de las políticas de la interfaz LAN. Con esta configuración se logra una gran flexibilidad en el criterio de selección del tráfico debido a que se utiliza una ACL (Access List Control) para seleccionar los paquetes que cumplan con el criterio del cliente, esto permite que se seleccionen paquetes dependiendo de la IP y red origen, IP y red destino, IP origen y destino simultáneamente, puertos utilizados, protocolo utilizado y el tiempo en que se ejecute el criterio de selección.

Debido a la gran flexibilidad en el criterio de selección de los paquetes que permite una mayor cantidad de alternativas para satisfacer los criterios de selección del cliente, además la facilidad para administrar y modificar la configuración del router se considera que el enrutamiento PBR es la mejor opción para cumplir con los objetivos del proyecto.

7. CARACTERÍSTICAS DE LA SEDE O LOCACIÓN

Con el objetivo de cumplir con una alta disponibilidad de los canales de comunicación de los clientes de la empresa Enercom se han realizado instalaciones de canales de back-up con iguales características que el canal principal para todas las sedes de producción logrando un respaldo y alta disponibilidad. Uno de los clientes observo que se tienen canales de back-up con iguales características que el principal pero pasivos en donde pueden pasar meses para que se utilice en una contingencia, de ahí parte la solicitud de que estos canales deben ser utilizados y aprovechados para beneficiar a los usuarios finales sin perder su esencia de canal de back-up.

Para cumplir con las exigencias del cliente se selecciona una locación de producción pequeña la cual cuenta con canal de back-up y principal de iguales características en donde se puede realizar las pruebas para implementar la configuración de un canal de back-up activo - activo con selección de tráfico. La sede seleccionada es La Creciente. En la figura 9 se muestra la topología de la sede La Creciente … Véase numeral 7.1 …

El canal principal comunica la sede de Bogotá con la locación de producción La Creciente, en este canal se utiliza el servicio de un ISP y un saltos o puntos repetidores a través de enlaces microondas para completar el canal entre las dos sede, el canal de back-up se implementa utilizando un segundo proveedor ISP y un solo salto o repetidor con enlaces microondas, el canal de back-up llega a Bogotá a una sede alterna del cliente, ambos canales tienen un ancho de banda de 4 Mbps.

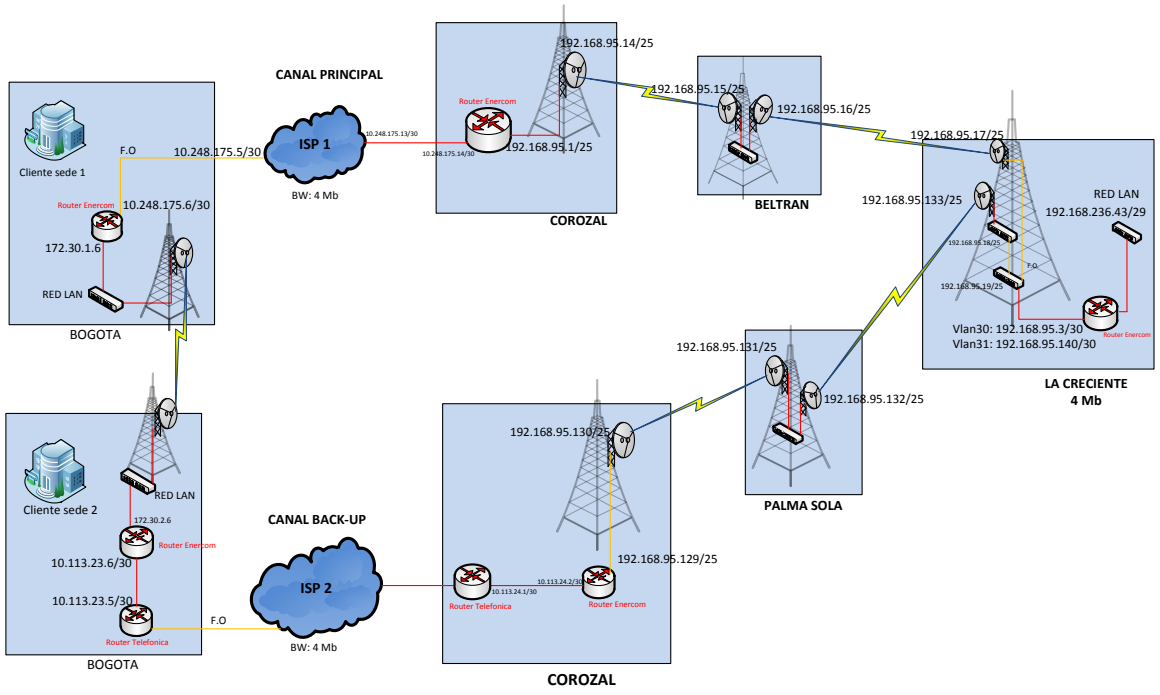
La ruta principal inicia en la sede de Bogotá, se conecta con el ISP 1 hasta la sede de Enercom en Corozal, desde este punto el canal continúa a través de radios microondas hasta el cerro Beltran y por último se comunica con la sede de La Creciente. La ruta de back-up inicia en la sede alterna en Bogotá, se conecta a través del ISP 2 llegando al municipio de Corozal, luego por radios

microondas se conecta con el cerro Palma sola y por último a través de enlace microondas con la sede de La Creciente.

7.1 TOPOLOGÍA SEDE LA CRECIENTE

En la figura 9 se muestra la topología de red de la sede La Creciente que fue la locación o sede seleccionada para implementar la configuración.

Figura 9. Topología La Creciente



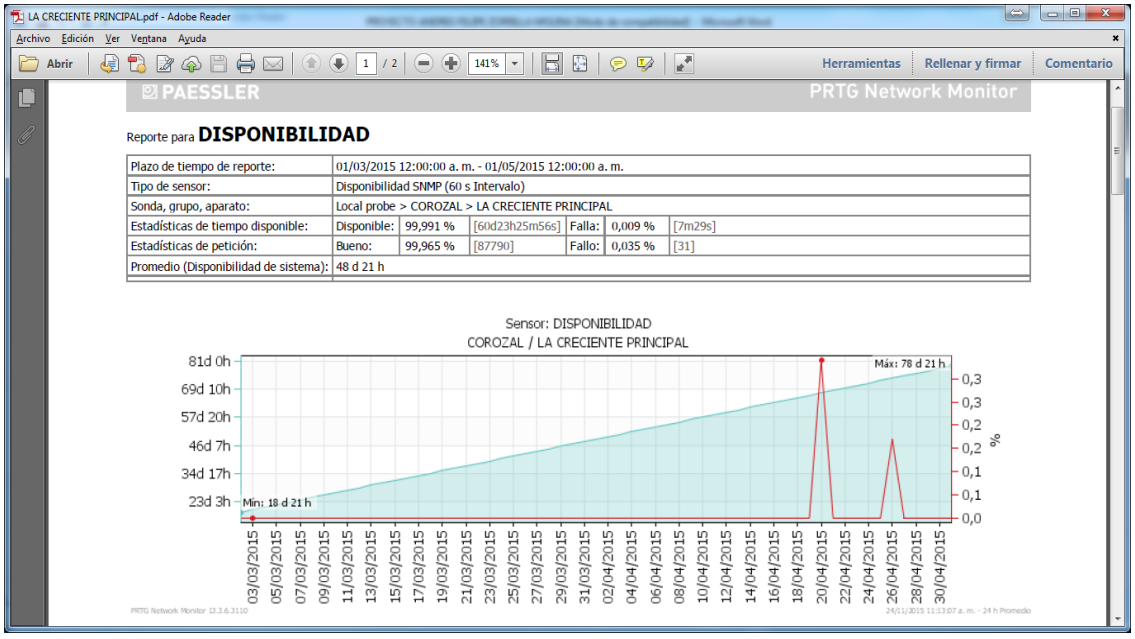
Fuente. Enercom S.A

8. CRITERIO DE SELECCIÓN DEL CLIENTE

En reuniones sostenidas con el cliente este informa que para ellos el tráfico más importante que se transporta sobre la red es el de aplicativos corporativos como los financieros, de perforación, telemetría, voz IP y chat interno corporativo. El tráfico hacia internet tiene una prioridad secundaria.

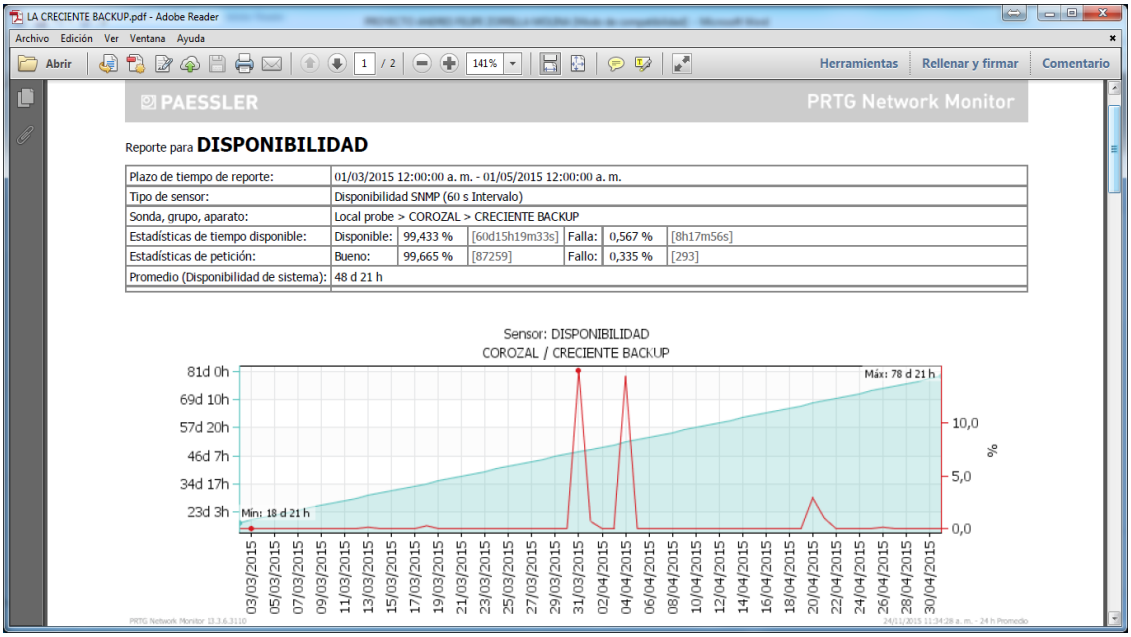
Se establece que para la prueba inicial en la sede La Creciente el tráfico más relevante para la empresa debe ir por la ruta que ha demostrado mayor confiabilidad y estabilidad en el servicio. Para confirmar cuál de los dos canales tiene un mejor desempeño nos apoyamos con la herramienta de monitoreo PRTG la cual monitorea constantemente el desempeño de los dos canales, se realiza una consulta de la disponibilidad del servicio entre el primero de marzo y el primero de mayo de 2015 y se determina que la ruta principal cuenta con mayor disponibilidad que la ruta de back-up, para el primero se tiene una disponibilidad del 99.99%, ver figura 10, y para el segundo una disponibilidad del 99.43%, ver figura 11.

Figura 10. Disponibilidad canal principal



Fuente. Enercom S.A

Figura 11. Disponibilidad canal de back-up



Fuente. Enercom S.A

Con ayuda del administrador de red del cliente se define como criterio técnico de selección que todos los paquetes que tengan como IP destino los servidores en Bogotá deben de ser enrutados por el canal con mejora disponibilidad. Las redes IP de los servidores en Bogotá son las siguientes:

10.201.0.0/16 red de servidores
10.202.0.0/16 red de servidores
10.203.0.0/16 red de servidores
10.204.0.0/16 red de servidores
10.205.0.0/16 red de servidores
10.230.0.0/16 red de servidores

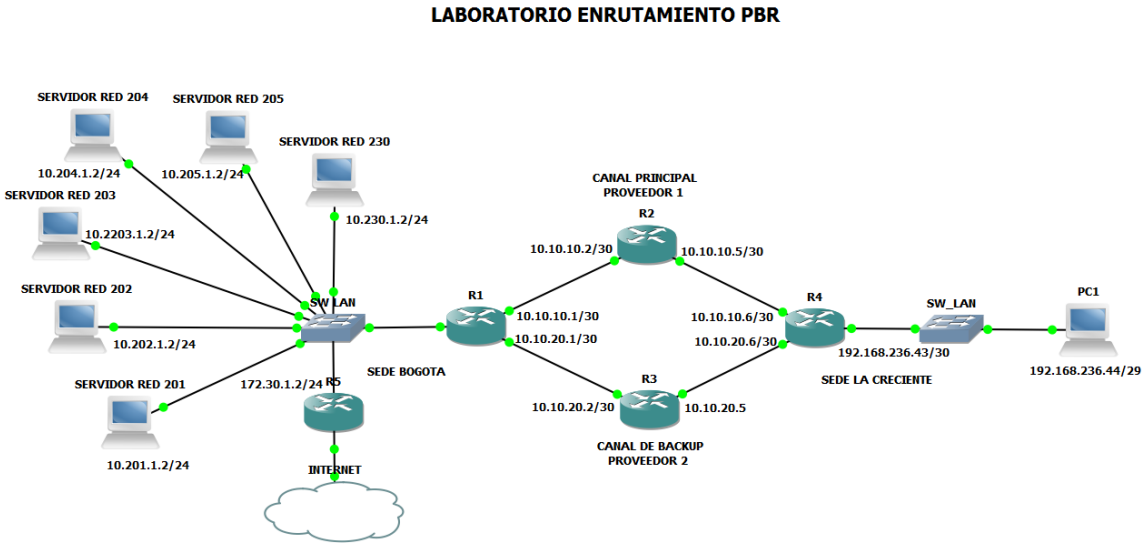
Este es el criterio de selección definido por el cliente para distribuir el tráfico entre el canal principal y el canal de back-up.

9. PRUEBAS DE LABORATORIO

El objetivo del laboratorio es probar si la configuración que se implementará en la red del cliente logra cumplir el objetivo de tener un canal de back-up activo – activo con la posibilidad de selección de tráfico. Para este laboratorio se utiliza el software GNS3 que permite simular el funcionamiento de enrutadores Cisco en una red determinada.

En este laboratorio se utiliza la topología de red de la figura 12 que simula la conexión entre la sede principal en Bogotá y la sede de producción La Creciente, en esta red se utilizan dos rutas para comunicar ambos extremos, la topología de red para el laboratorio es la siguiente:

Figura 12. Topología laboratorio enrutamiento



Fuente. El autor

En la parte izquierda de la topología se simula la red de Bogotá en donde se encontraran 6 redes de servidores y una conexión de hacia internet, según el criterio técnico definido por el cliente el tráfico relevante es el que tiene como destino la red de los servidores que permite a los usuarios utilizar aplicativos corporativos de producción, financieros, voz IP, etc. Cuando los dos canales están activos este tráfico debe tomar la ruta principal y el tráfico hacia internet debe tomar la ruta

de back-up consiguiendo la distribución del tráfico por las dos rutas. Si una de las dos rutas no está operativa todo el tráfico debe conmutar automáticamente hacia la ruta que esta operativa. En la parte derecha de la topología se simula la red de La Creciente donde se encuentran los usuarios finales que utilizaran los canales de comunicación para obtener los servicios de aplicativos corporativos e Internet.

Para logra el objetivo del laboratorio en el router R4 se configura el monitoreo de las dos rutas principal y back-up para determinar su operatividad, además se configuran rutas estáticas para que el monitoreo de estas redes siempre se realice por la misma ruta.

```
ip sla 1
 icmp-echo 10.10.10.1 source-interface FastEthernet0/0
 threshold 100
 frequency 10
ip sla schedule 1 life forever start-time now
ip sla 2
 icmp-echo 10.10.20.1 source-interface FastEthernet1/0
 threshold 100
 frequency 10
ip sla schedule 2 life forever start-time now
!
ip route 10.10.10.1 255.255.255.255 10.10.10.5 name Ruta_mon_isp_1
ip route 10.10.20.1 255.255.255.255 10.10.20.5 name Ruta_mon_isp_2
```

Se configura el comando Track para determinar el estado de los IP SLA.

```
track 1 ip sla 1 reachability
!
```

track 2 ip sla 2 reachability

Se configuran las rutas estáticas por defecto condicionadas por el estado de los tracks.

ip route 0.0.0.0 0.0.0.0 10.10.10.5 10 name RUTA_INTERNET_ISP1 track 1

ip route 0.0.0.0 0.0.0.0 10.10.20.5 name RUTA_INTERNET_ISP2 track 2

La ruta de internet por el ISP 1 tiene un peso adiciona de (10) para asegurar que si las dos rutas están activas solo una entre a la tabla de enrutamiento, en este caso entraría la ruta por el ISP 2 que es el canal de back-up. Con esto se logra que cuando las dos rutas estén activas el tráfico de internet tome la ruta de back-up.

Se configura una lista de acceso para seleccionar los paquetes que tienen como destino los servidores del cliente.

ip access-list extended SERVIDOR

permit ip any 10.201.1.0 0.0.0.255

permit ip any 10.202.1.0 0.0.0.255

permit ip any 10.203.1.0 0.0.0.255

permit ip any 10.204.1.0 0.0.0.255

permit ip any 10.205.1.0 0.0.0.255

permit ip any 10.230.1.0 0.0.0.255

!

Luego se crea un Route-map para determinar el siguiente salto de los paquetes seleccionados por la lista de acceso.

```
route-map PRINCIPAL permit 10
 match ip address SERVIDOR
 set ip next-hop verify-availability 10.10.10.5 1 track 1
 set ip next-hop 10.10.20.5
!
```

Por último en la interfaz LAN se incluye una instrucción para ejecutar el Route-map.

```
interface FastEthernet2/0
 description CONEXION LAN LA CRECIENTE
 ip address 192.168.236.43 255.255.255.248
 ip policy route-map PRINCIPAL
 duplex full
```

La configuración completa de los routers R1 y R4 es la siguiente.

Router R1

```
R1#SH RUN
!
hostname R1
!
track 1 ip sla 1 reachability
!
track 2 ip sla 2 reachability
!
interface FastEthernet0/0
 no ip address
 duplex full
!
interface FastEthernet0/0.10
 description RED SERVIDOR 1
 encapsulation dot1Q 10
 ip address 10.201.1.1 255.255.255.0
 ip policy route-map PRINCIPAL
!
interface FastEthernet0/0.20
```

```
 description RED SERVIDOR 2
 encapsulation dot1Q 20
 ip address 10.202.1.1 255.255.255.0
 ip policy route-map PRINCIPAL
!
interface FastEthernet0/0.30
 description RED SERVIDOR 3
 encapsulation dot1Q 30
 ip address 10.203.1.1 255.255.255.0
 ip policy route-map PRINCIPAL
!
interface FastEthernet0/0.40
 description RED SERVIDOR 4
 encapsulation dot1Q 40
 ip address 10.204.1.1 255.255.255.0
 ip policy route-map PRINCIPAL
!
interface FastEthernet0/0.50
 description RED SERVIDOR 5
 encapsulation dot1Q 50
 ip address 10.205.1.1 255.255.255.0
```

```
 ip policy route-map PRINCIPAL
!
interface FastEthernet0/0.51
 description RED SERVIDOR 6
 encapsulation dot1Q 51
 ip address 10.230.1.1 255.255.255.0
 ip policy route-map PRINCIPAL
!
interface FastEthernet0/0.52
 description CONEXION A INTERNET
 encapsulation dot1Q 52
 ip address 172.30.1.1 255.255.255.0
!
interface FastEthernet1/0
 description WAN PROVEEDOR 1
 ip address 10.10.10.1 255.255.255.252
 duplex full
!
interface FastEthernet2/0
 description WAN PROVEEDOR 2
 ip address 10.10.20.1 255.255.255.252
```

```
 duplex full
!
ip route 192.168.236.40 255.255.255.248 10.10.10.2 10 name LA_CRECIENTE_ISP_1 track 1
ip route 192.168.236.40 255.255.255.248 10.10.20.2 name LA_CRECIENTE_ISP_2 track 2
ip route 0.0.0.0 0.0.0.0 172.30.1.2 name RUTA_DEFAULT
ip route 10.10.10.6 255.255.255.255 10.10.10.2 name ruta_mon_isp_1
ip route 10.10.20.6 255.255.255.255 10.10.20.2 name ruta_mon_isp_2
!
ip access-list extended SERVIDOR
 permit ip 10.201.1.0 0.0.0.255 192.168.236.40 0.0.0.7
 permit ip 10.202.1.0 0.0.0.255 192.168.236.40 0.0.0.7
 permit ip 10.203.1.0 0.0.0.255 192.168.236.40 0.0.0.7
 permit ip 10.204.1.0 0.0.0.255 192.168.236.40 0.0.0.7
 permit ip 10.205.1.0 0.0.0.255 192.168.236.40 0.0.0.7
 permit ip 10.230.1.0 0.0.0.255 192.168.236.40 0.0.0.7
!
ip sla 1
 icmp-echo 10.10.10.6 source-interface FastEthernet1/0
 threshold 100
 frequency 10
ip sla schedule 1 life forever start-time now
```

```
ip sla 2
 icmp-echo 10.10.20.6 source-interface FastEthernet2/0
 threshold 100
 frequency 10
ip sla schedule 2 life forever start-time now
!
route-map PRINCIPAL permit 10
 match ip address SERVIDOR
 set ip next-hop verify-availability 10.10.10.2 1 track 1
 set ip next-hop 10.10.20.2
!
!
end
R1#
```

Router R4

```
R4#SH RUN
!
hostname R4
!
track 1 ip sla 1 reachability
```

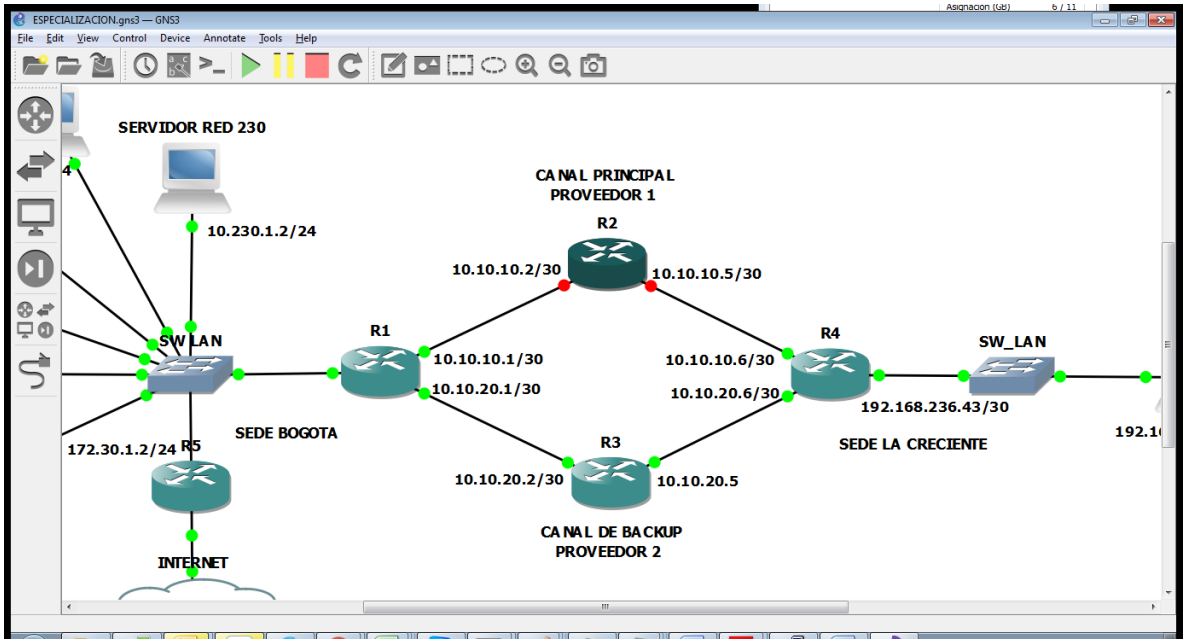
```
!
track 2 ip sla 2 reachability
!
interface FastEthernet0/0
 description CONEXION CON PROVEEDOR 1
 ip address 10.10.10.6 255.255.255.252
 duplex full
!
interface FastEthernet1/0
 description CONEXION CON PROVEEDOR 2
 ip address 10.10.20.6 255.255.255.252
 duplex full
!
interface FastEthernet2/0
 description CONEXION LAN LA CRECIENTE
 ip address 192.168.236.43 255.255.255.248
 ip policy route-map PRINCIPAL
 duplex full
!
ip route 0.0.0.0 0.0.0.0 10.10.10.5 10 name RUTA_INTERNET_ISP1 track 1
ip route 0.0.0.0 0.0.0.0 10.10.20.5 name RUTA_INTERNET_ISP2 track 2
```

```
ip route 10.10.10.1 255.255.255.255 10.10.10.5 name Ruta_mon_isp_1
ip route 10.10.20.1 255.255.255.255 10.10.20.5 name Ruta_mon_isp_2
!
ip access-list extended SERVIDOR
 permit ip any 10.201.1.0 0.0.0.255
 permit ip any 10.202.1.0 0.0.0.255
 permit ip any 10.203.1.0 0.0.0.255
 permit ip any 10.204.1.0 0.0.0.255
 permit ip any 10.205.1.0 0.0.0.255
 permit ip any 10.230.1.0 0.0.0.255
!
ip sla 1
 icmp-echo 10.10.10.1 source-interface FastEthernet0/0
 threshold 100
 frequency 10
ip sla schedule 1 life forever start-time now
ip sla 2
 icmp-echo 10.10.20.1 source-interface FastEthernet1/0
 threshold 100
 frequency 10
ip sla schedule 2 life forever start-time now
```

```
!
route-map PRINCIPAL permit 10
 match ip address SERVIDOR
 set ip next-hop verify-availability 10.10.10.5 1 track 1
 set ip next-hop 10.10.20.5
!
R4#
```

Inicialmente se ejecutaron pruebas para determinar si el canal de back-up y el canal principal se respaldan mutuamente, si uno de los dos canales no está operativo todo el tráfico debe ser enviado por el canal activo. Para simular la caída del canal principal se apaga el router R2, como se muestra en la figura 13, con lo cual solo queda activa la ruta de back-up.

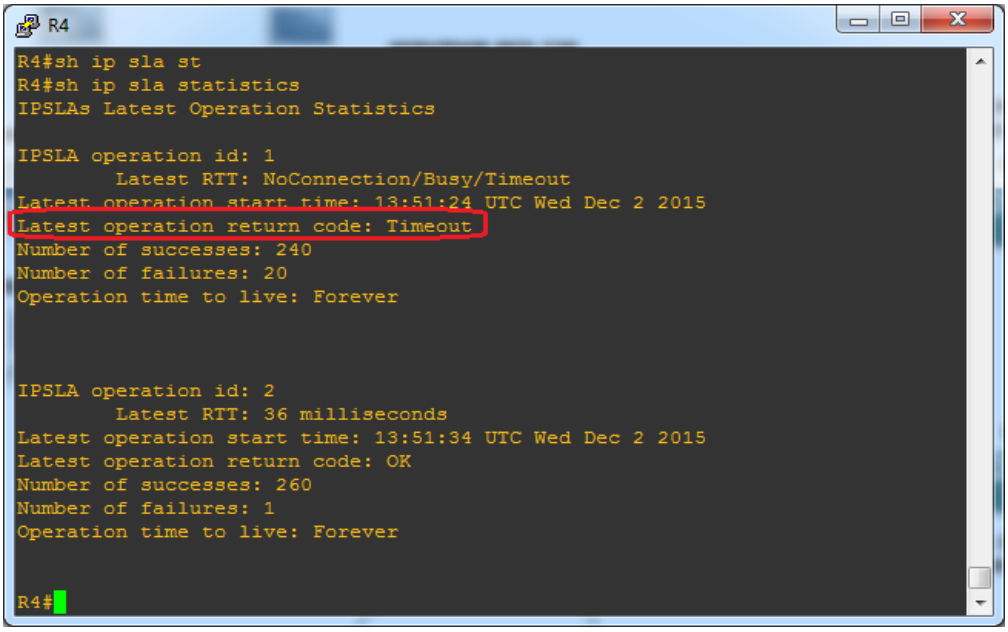
Figura 13. Topología de laboratorio con el canal principal caído



Fuente. El autor

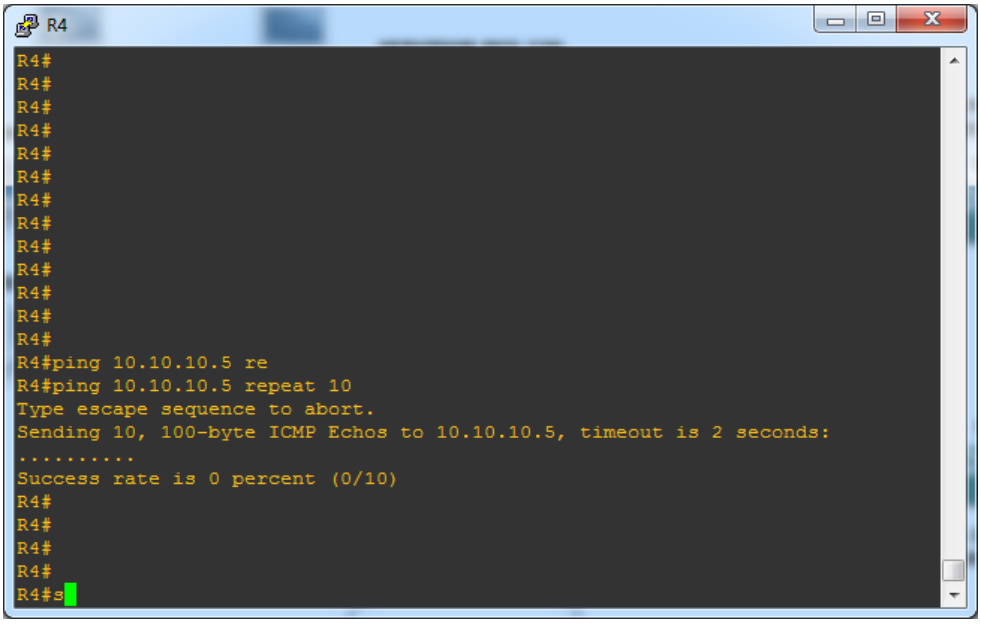
Se verifica la caída de la ruta principal haciendo una prueba de ping desde el router R4 y verificando el estado de los IP SLA que monitorean las rutas, como se muestra en la figura 14 y 15.

Figura 14. Verificación de caída del canal principal



Fuente. El autor

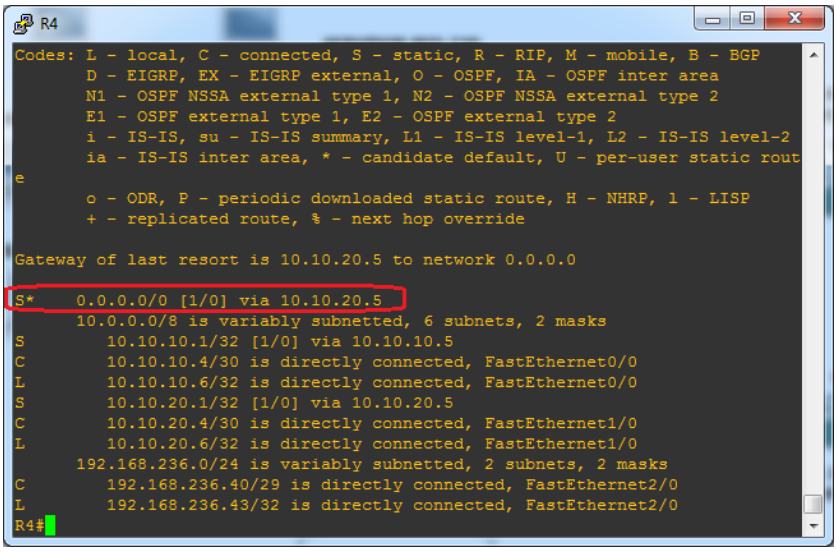
Figura 15. Prueba de ping para verificar caída del canal principal



Fuente. El autor

Se verifica la tabla de enrutamiento para confirmar que la ruta por defecto este enrutando los paquetes hacia el canal de back-up, ver figura 16.

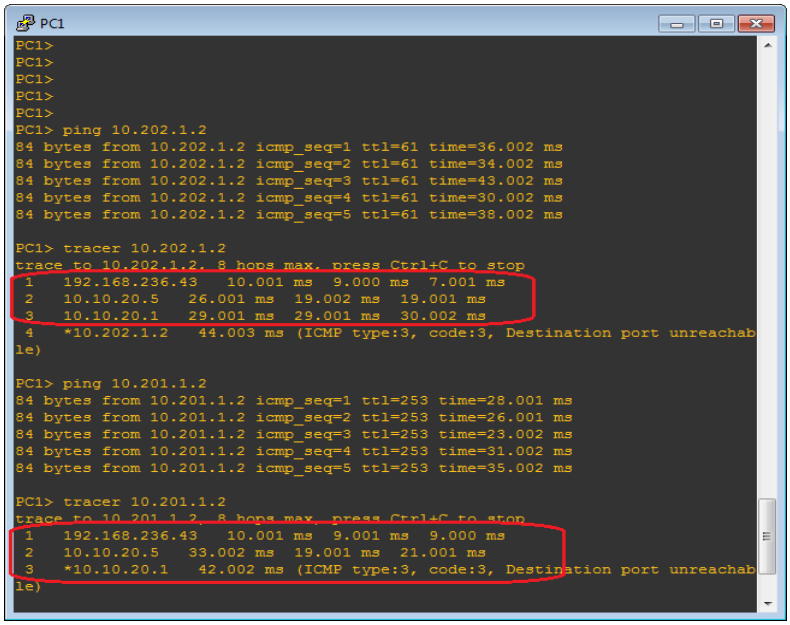
Figura 16. Ruta por defecto hacia el canal de back-up



Fuente. El autor

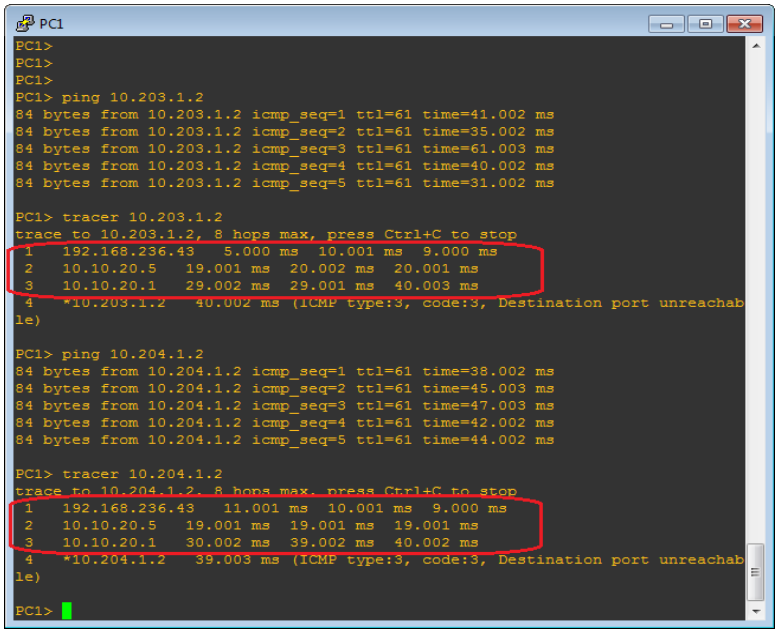
Se realizan pruebas de ping y trazas desde el PC1, como se observa en la figura 17, 18 y 19, para confirmar que la comunicación con los servidores y hacia internet tome la ruta de back-up.

Figura 17. Pruebas hacia ruta de back-up 1



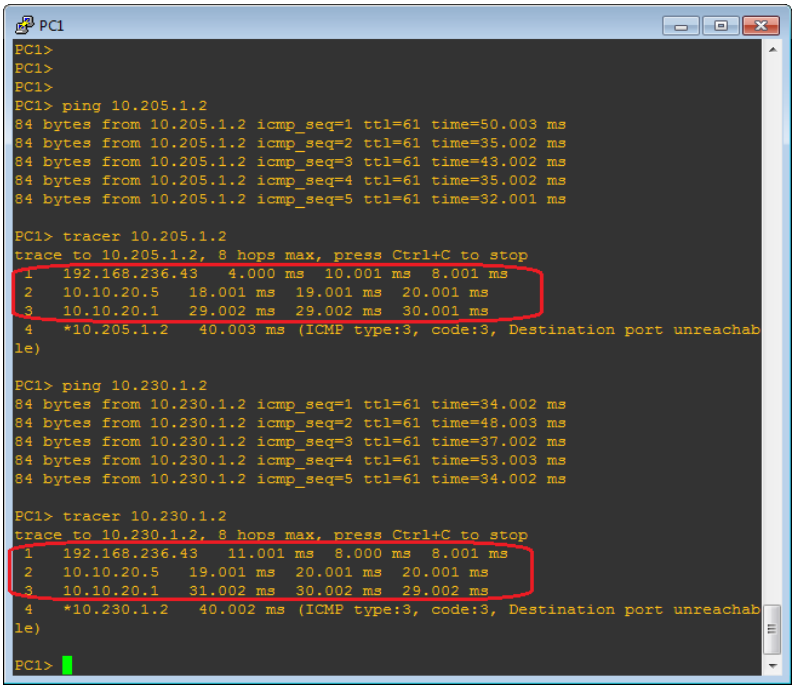
Fuente. El autor

Figura 18. Pruebas hacia ruta de back-up 2



Fuente. El autor

Figura 19. Pruebas hacia ruta de back-up 3

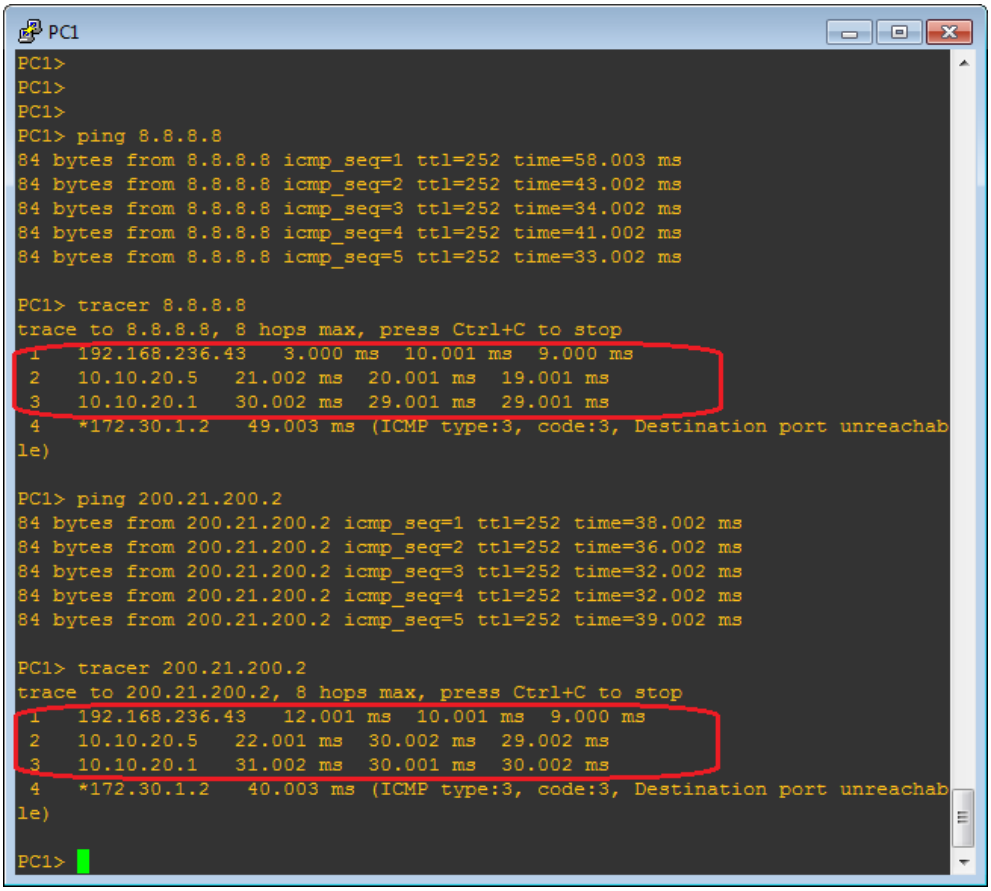


Fuente. El autor

En las figuras anteriores se observa que al hacer un seguimiento de los saltos que toman los paquetes con destino a la red de servidores (10.230.1.2, 10.205.1.2, 10.204.1.2, 10.203.1.2, 10.202.1.2, 10.201.1.2) en todas las imágenes coincide que el segundo salto es el router con IP 10.10.20.5 que corresponde al canal de back-up proveedor 2, con esto se confirma que los paquetes utilizan el canal de back-up para llegar al destino.

Para probar el servicio de internet se configuran dos IPs públicas en el router R5 para simular el servicio de internet, desde el PC1 se verifica conectividad haciendo una prueba de ping y se confirma la ruta que toman los paquetes con una traza, ver figura 20.

Figura 20. Pruebas hacia ruta de back-up 4

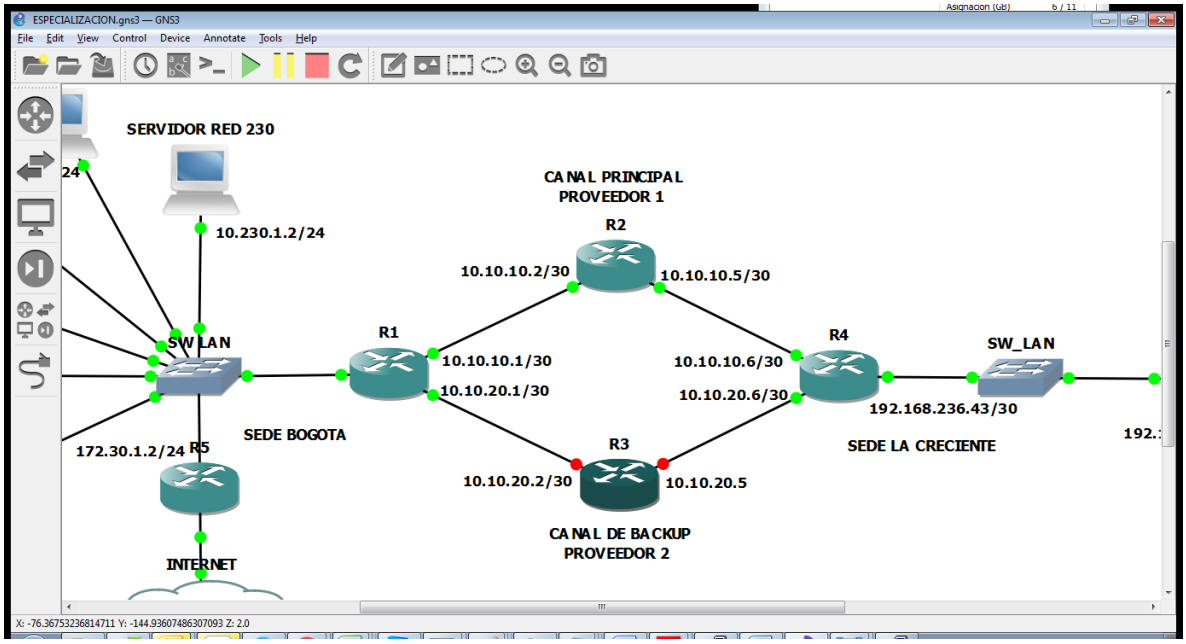


Fuente. El autor

Como se observa en las figuras 17 a la 19 todos los paquetes toman la ruta con IP 10.10.20.5 y 10.10.20.1 correspondiente al canal de back-up, con esto se confirma que si el canal principal no está operativo todo el tráfico conmuta automáticamente al canal de back-up.

Para la siguiente prueba se restablece el canal principal y se apaga el router R3, como se muestra en la figura 21, para simular la falla del canal de back-up.

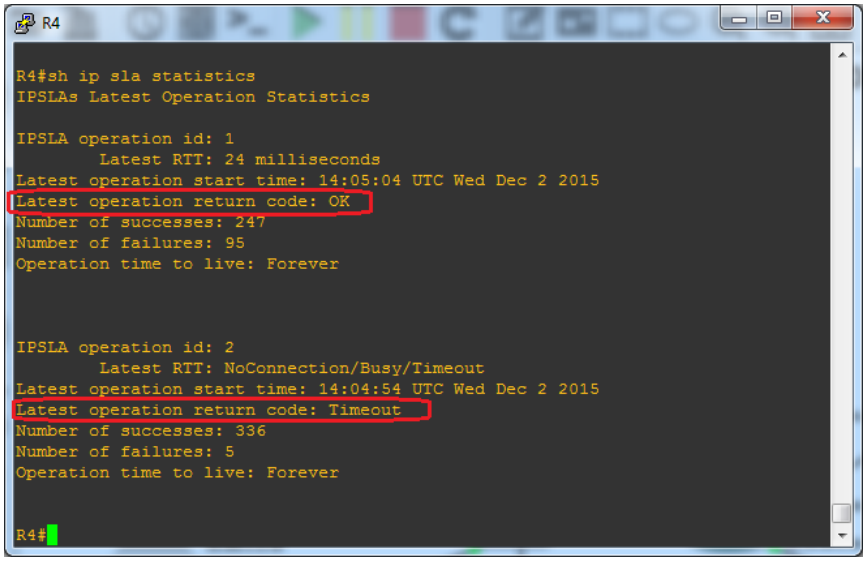
Figura 21. Topología de laboratorio con el canal de back-up caído



Fuente. El autor

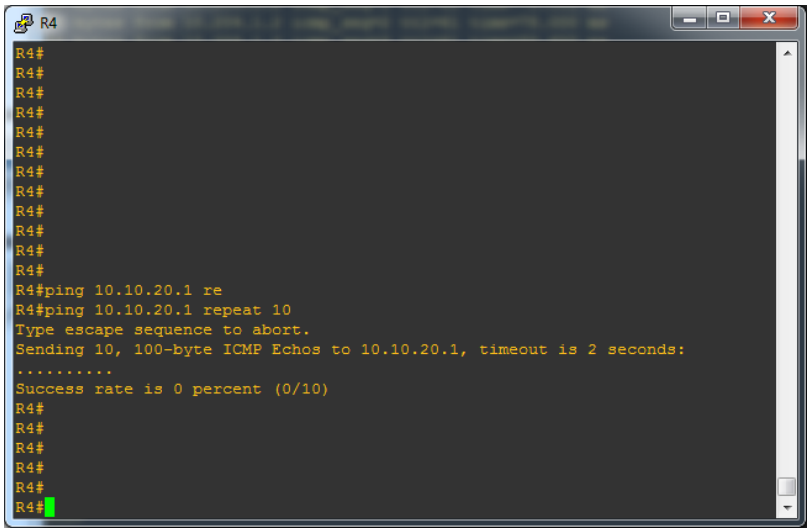
Se verifica la caída de la ruta de back-up haciendo una prueba de ping desde el router R4 y verificando el estado de los IP SLA que monitorean las rutas, ver figura 22 y 23.

Figura 22. Verificación de caída del canal de back-up



Fuente. El autor

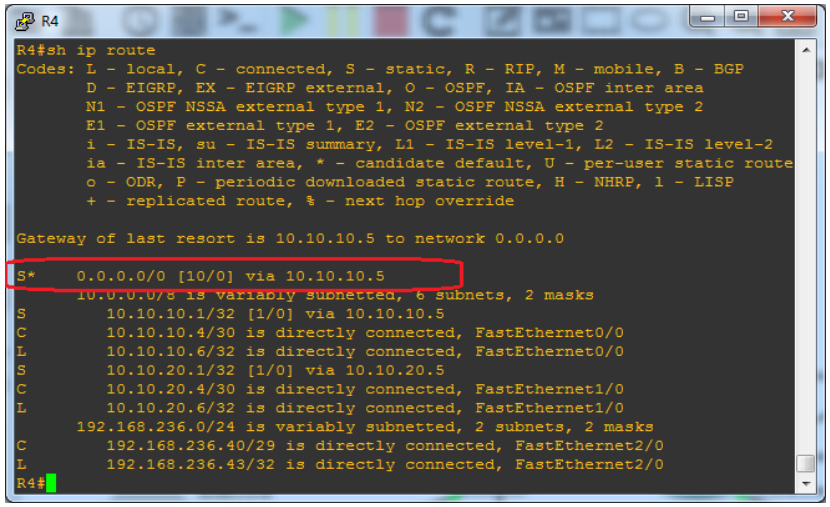
Figura 23. Prueba de ping para verificar caída del canal de back-up



Fuente. El autor

Como se muestra en la figura 24 se verifica la tabla de enrutamiento para confirmar que la ruta por defecto este enrutando los paquetes hacia el canal de principal IP 10.10.10.5.

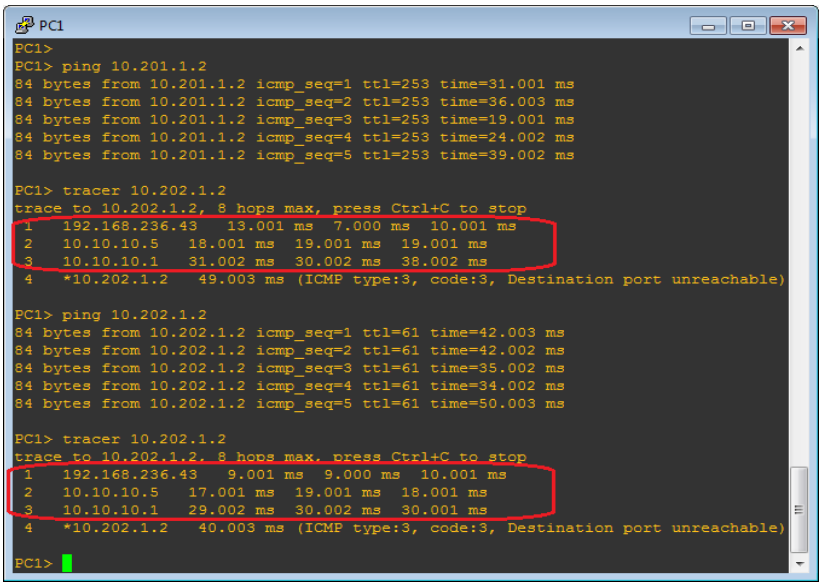
Figura 24. Ruta por defecto hacia el canal principal



Fuente. El autor

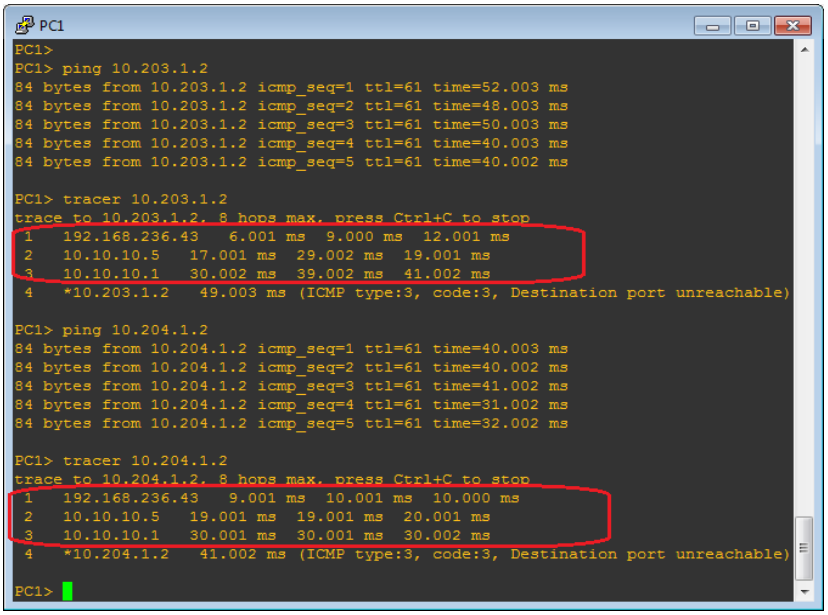
Se realizan pruebas de ping y trazas para confirmar que la comunicación con los servidores y hacia Internet se envíe por la ruta principal con la IP 10.10.10.5, ver figuras 25 a la 28.

Figura 25. Pruebas hacia ruta principal 1



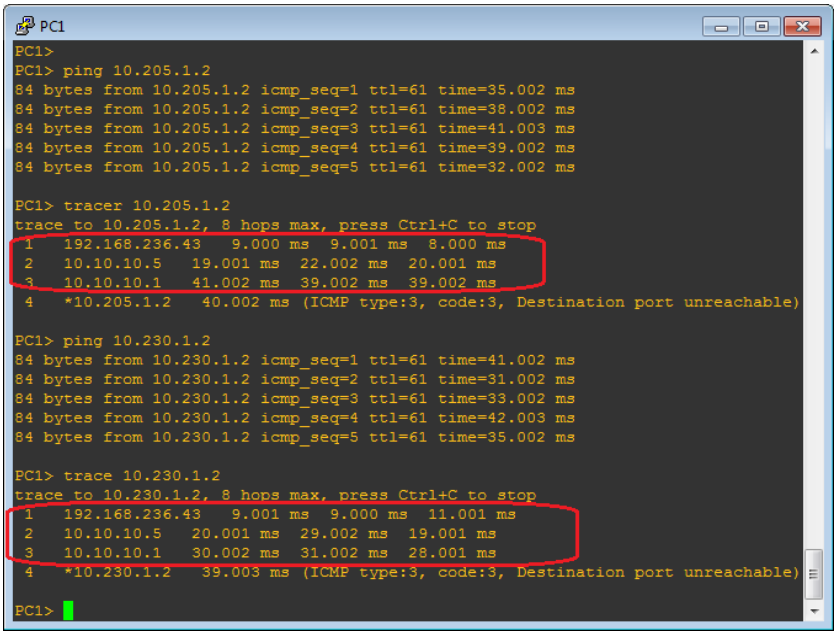
Fuente. El autor

Figura 26. Pruebas hacia ruta principal 2



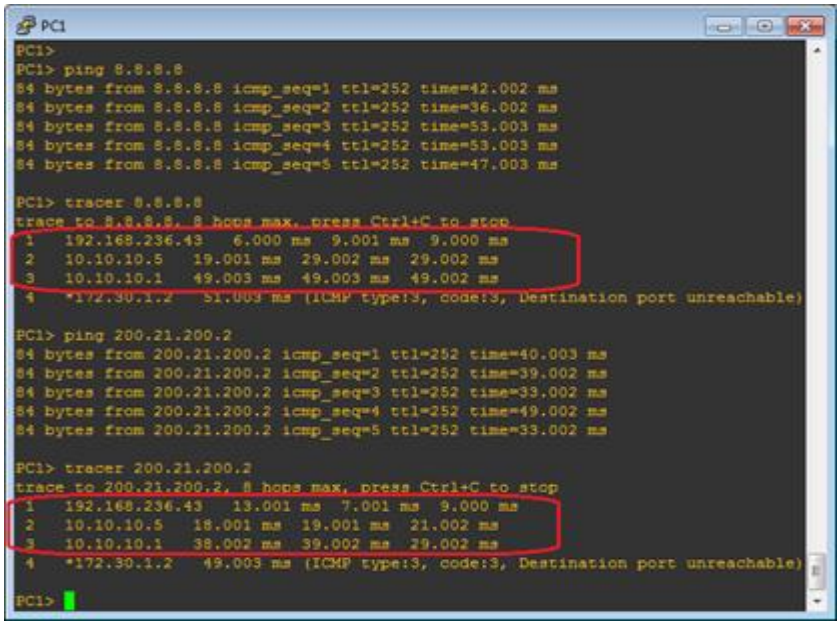
Fuente. El autor

Figura 27. Pruebas hacia ruta principal 3



Fuente. El autor

Figura 28. Pruebas hacia ruta principal 4



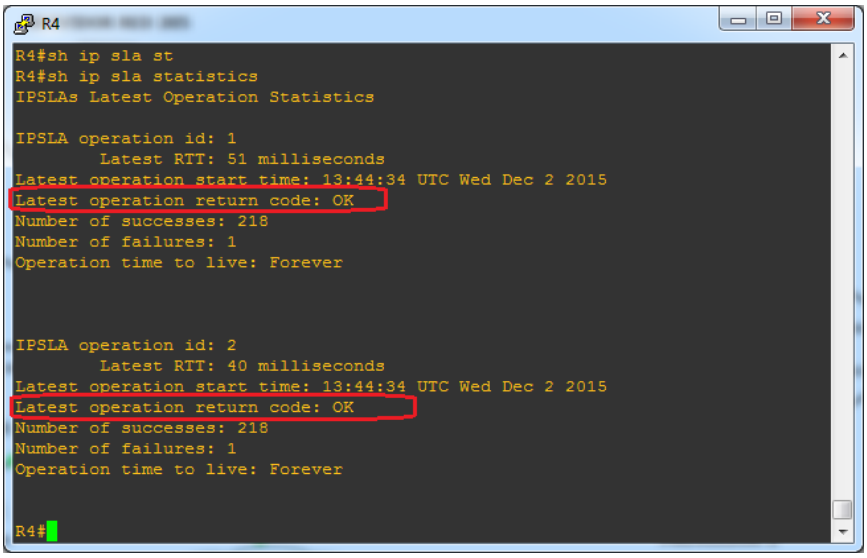
Fuente. El autor

En las figuras anteriores se observa que al hacer un seguimiento de los saltos que toman los paquetes con destino a la red de servidores (10.230.1.2, 10.205.1.2, 10.204.1.2, 10.203.1.2, 10.202.1.2, 10.201.1.2) en todas las imágenes coincide que el segundo salto es el router con IP 10.10.10.5 que corresponde al canal de principal proveedor 1, con esto se confirma que los paquetes utilizan el canal principal para llegar al destino.

Con estas pruebas se demuestra que cuando el canal de back-up no está operativo todos los paquetes toman la ruta del canal principal demostrando que ambos canales se respaldan mutuamente. Ahora se realizaran pruebas con los dos canales activos para verificar que se distribuya el tráfico según lo exigido por el cliente, los paquetes hacia las redes de los servidores deben tomar la ruta principal y los paquetes que tiene como destino redes distintas a las de los servidores deben tomar la ruta de back-up.

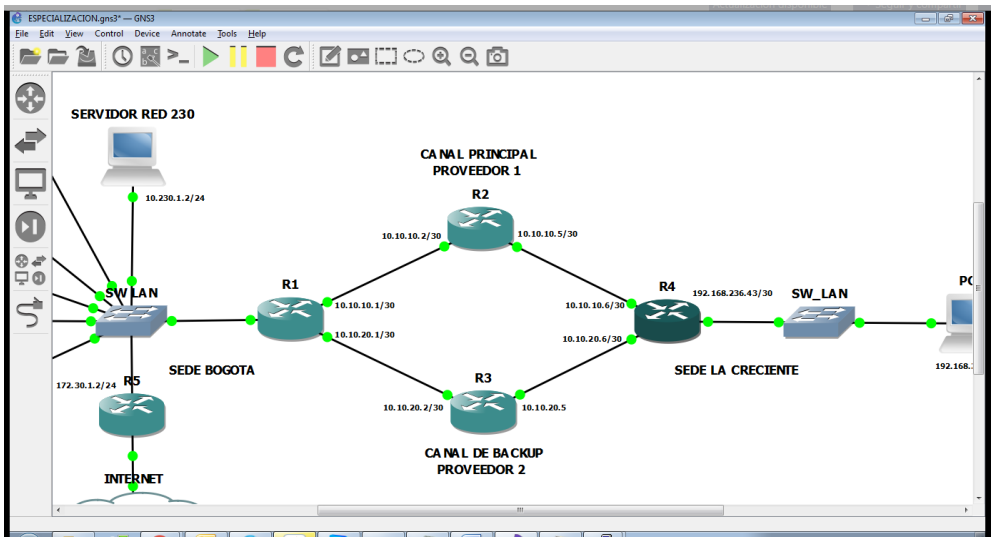
Como se muestra en la figura 29 y 30 se confirma que las dos rutas estén operativas.

Figura 29. Verificación del canal de back-up y principal operativos



Fuente. El autor

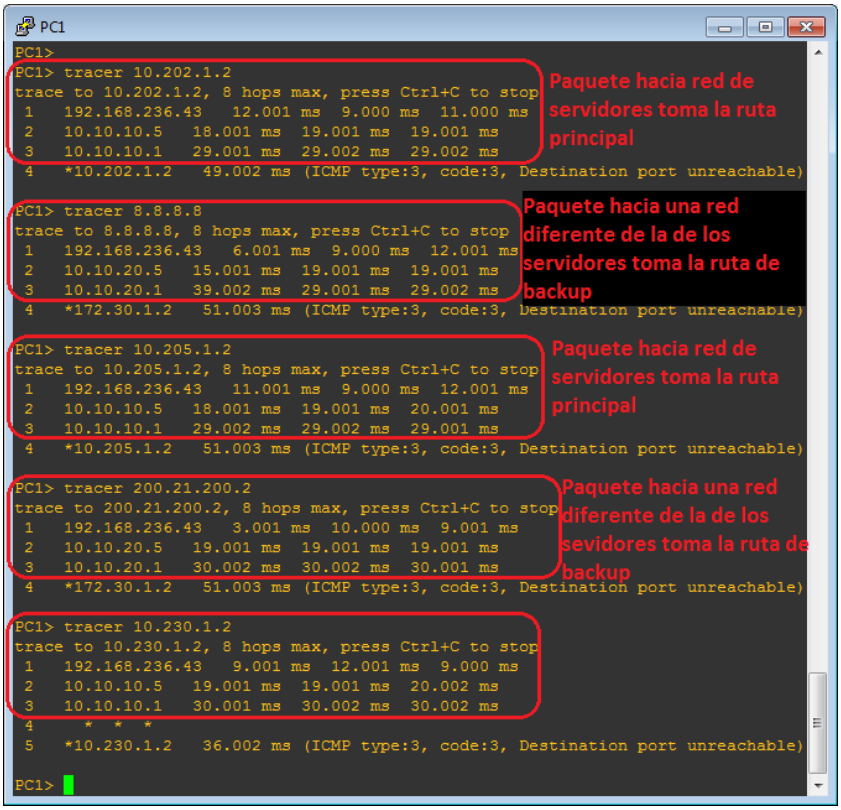
Figura 30. Topología de laboratorio con el canal back-up y principal operativos



Fuente. El autor

Se realizan trazas hacia las redes de los servidores para verificar los saltos que toman los paquetes y luego se realizan trazas hacia redes diferentes que las de los servidores para verificar que ruta toman. El resultado de esta prueba se observa en la figura 31.

Figura 31. Trazas para verificar distribución de tráfico



Fuente. El autor

En la figura anterior se observa que al hacer un seguimiento de los saltos que toman los paquetes con destino a la red de servidores (10.230.1.2, 10.205.1.2, 10.204.1.2, 10.203.1.2, 10.202.1.2, 10.201.1.2) en todos los seguimientos coincide que el segundo salto es el router con IP 10.10.10.5 que corresponde al canal principal proveedor 1, el seguimiento a los paquetes con destino la IP 8.8.8.8 hace su segundo salto por la IP 10.10.20.5 que corresponde al canal de back-up proveedor 2.

Con estas pruebas se confirma que la configuración de enrutamiento PBR aplicada en los routers del simulador GNS permite la distribución de tráfico por las dos rutas y además los dos canales se respaldan mutuamente logrando el objetivo de un canal de back-up activo-activo con selección de tráfico.

10. IMPLEMENTACIÓN DE LA SOLUCIÓN

10.1 PUESTA EN MARCHA DE LA CONFIGURACIÓN

Para realizar la implementación de la configuración que permitirá tener un canal de back-up activo-activo con selección de tráfico se solicita una ventana de mantenimiento de dos horas con el cliente. Lo primero que se realiza es configurar en el router de la sede La Creciente el monitoreo de la ruta principal y la ruta de back-up utilizando la herramienta IP SLA, con esto se conoce en qué momento alguna de las dos rutas falla para conmutar todo el tráfico hacia la ruta activa. Según la topología de la Figura 9 … Véase numeral 7.1 … desde el router de La Creciente se debe monitorea las IP 10.248.175.6 para la ruta principal y la IP 10.113.23.6 para la ruta de back-up.

```
ip sla monitor 3
 type echo protocol ipIcmpEcho 10.248.175.6 source-interface FastEthernet0/1.30
 timeout 1000
 threshold 400
 frequency 5
ip sla monitor schedule 3 life forever start-time now

ip sla monitor 10
 type echo protocol ipIcmpEcho 10.113.23.6 source-interface FastEthernet0/1.31
 timeout 1000
 threshold 400
```

frequency 5

ip sla monitor schedule 10 life forever start-time now

El comando "*ip sla monitor*" proporciona un número de identificación a la herramienta IP SLA, el comando "*type echo protocol ipIcmpEcho 10.248.175.6 source-interface FastEthernet0/1.30*" envía un paquete de prueba a la dirección IP 10.248.175.6 a través de la interfaz FastEthernet0/1.30 para determinar si esta IP responde y está activa, los comandos "*timeout, threshold y frequency*" proporcionan la frecuencia con la que se realiza la prueba y el tiempo de espera para recibir la respuesta, el comando "*ip sla monitor schedule 3 life forever start-time now*" proporciona los parámetro para saber desde que momento se inicia la prueba y hasta cuándo.

El monitoreo de estas dos IPs desde el router de La Creciente siempre se debe realizar a través de la misma ruta para garantizar un monitoreo efectivo de la ruta por lo que es necesario establecer en el enrutamiento una ruta específica para alcanza cada IP, se configura una ruta estática para alcanzar la IP 10.248.175.6 que corresponde al router de la sede 1 en Bogotá a través del router con IP 192.167.95.1 y para alcanzar la IP 10.113.23.6 que corresponde al router de la sede 2 en Bogotá a través del router con IP 192.168.95.129.

ip route 10.113.23.6 255.255.255.255 192.168.95.129

ip route 10.248.175.6 255.255.255.255 192.168.95.1

Para garantizar que en caso de que alguno de los dos canales falle todo el tráfico se envíe a través del canal activo desde el router de La Creciente se evalúa el estado de las rutas utilizando la herramienta Track, luego se condiciona el ingreso de la ruta a la tabla de enrutamiento dependiendo del resultado de la evaluación del comando Track. Si las dos rutas están activas se debe asegurar que solo una de ellas este en la tabla de enrutamiento y esto se logra agregando un

peso a la ruta de back-up, solo si la ruta principal no está en la tabla de enrutamiento la ruta de respaldo entra a la tabla de enrutamiento y en este caso todo el tráfico tomaría la ruta de back-up.

track 6 rtr 3 reachability

!

track 10 rtr 10 reachability

!

ip route 0.0.0.0 0.0.0.0 192.168.95.129 10 name RUTA_INTERNET_CANAL_BACKUP track 10

ip route 0.0.0.0 0.0.0.0 192.168.95.1 name RUTA_INTERNET_CANAL_PPAL track 6

Los comandos "*track 6 rtr 3 reachability*" y "*track 10 rtr 10 reachability*" realizan una evaluación al resultado de las pruebas de la herramienta IP SLA configurado anteriormente, el comando "*ip route 0.0.0.0 0.0.0.0 192.168.95.129 10 name RUTA_INTERNET_CANAL_BACKUP track 10*" es una ruta por defecto que solo ingresa a la tabla de enrutamiento si la evaluación del track 10 es positiva y si existe una ruta por defecto adicional esta no entrara a la tabla de enrutamiento porque tiene un peso adicional de 10, el comando "*ip route 0.0.0.0 0.0.0.0 192.168.95.1 name RUTA_INTERNET_CANAL_PPAL track 6*" es una ruta por defecto que solo ingresa a la tabla de enrutamiento si la evaluación del track 6 es positiva.

Hasta el momento esta es la configuración de una canal de back-up convencional que realiza una conmutación automática en caso de que la ruta principal falle, ahora se realiza la configuración para que el tráfico se distribuya dependiendo de la selección del cliente, para lograrlo debemos configurar una ACL (lista de control de acceso) en el router de La Creciente que nos permita capturar el tráfico seleccionado por el cliente, se configura una ACL con el criterio técnico determinado por el administrador de red del cliente … Véase numeral 8 ….

```
ip access-list extended SERVIDORES
 permit ip any 10.201.0.0 0.0.255.255
 permit ip any 10.202.0.0 0.0.255.255
 permit ip any 10.203.0.0 0.0.255.255
 permit ip any 10.204.0.0 0.0.255.255
 permit ip any 10.205.0.0 0.0.255.255
 permit ip any 10.230.0.0 0.0.255.255
```

La configuración anterior selecciona todos los paquetes que tienen como destino la red de servidores del cliente (10.201.0.0, 10.202.0.0, 10.203.0.0, 10.204.0.0, 10.205.0.0 y 10.230.0.0).

Luego en el router de La Creciente se crea un Route Map que permite enrutar el tráfico seleccionado por la ruta que desee el cliente.

```
route-map PRINCIPAL permit 10
 match ip address SERVIDORES
 set ip next-hop verify-availability 192.168.95.1 1 track 6
 set ip next-hop 192.168.95.129
```

En este route map los paquetes que coinciden con la lista de acceso "*SERVIDORES*" son enviados por la ruta principal si la evaluación que realiza el track 6 es positiva, lo que confirma que la ruta principal esta operativa, esto se logra con el comando "*set ip next-hop verify-availability*

192.168.95.1 1 track 6", de lo contrario enviarán los paquetes por la ruta de back-up con el comando "*set ip next-hop 192.168.95.129*".

En la interfaz LAN del router de La Creciente se incluye la política para invocar el route map y con esto se asegura que todos los paquetes que se originan en la LAN son evaluados para determinar que ruta deben tomar, esto se logra con el comando "*ip policy route-map PRINCIPAL*".

```
interface FastEthernet0/0
 description CONEXION LAN
 ip address 192.168.236.43 255.255.255.248
 ip policy route-map PRINCIPAL
 load-interval 30
 speed auto
 full-duplex
!
```

Para finalizar de acuerdo con la solicitud del cliente el tráfico que no es relevante debe de tomar la ruta menos confiable, por lo tanto se modifican las rutas estáticas en el router de La Creciente para que cuando los dos canales estén activos la ruta por defecto sea el canal de back-up, se coloca peso a la ruta principal para que sea la ruta del canal de back-up la que ingrese a la tabla de enrutamiento.

```
ip route 0.0.0.0 0.0.0.0 192.168.95.129 name RUTA_INTERNET_CANAL_BACKUP track 10
```

ip route 0.0.0.0 0.0.0.0 192.168.95.1 10 name RUTA_INTERNET_CANAL_PPAL track 6

Con esta configuración se logra inicialmente monitorear las dos rutas principal y back-up para determinar su operatividad y se condiciona la tabla de enrutamiento con dos rutas por defecto que determinan por cuál de las dos enviará el tráfico menos relevante, con la configuración de la política route map en la interfaz LAN se seleccionan los paquetes que coinciden con el criterio de selección del cliente para determinar cuál de las dos rutas utilizar.

Cuando las dos rutas están activas y llega un paquete que coincide con el criterio de selección del cliente el route map envía este paquete por la ruta principal, pero si llega un paquete que no coincide con el criterio de selección este se reenvía dependiendo de las rutas de la tabla de enrutamiento la cual determinará enviar este paquete por el canal de back-up. Con esto se logra que solo el tráfico que es relevante para el cliente tome la ruta más confiable que es el canal principal y el resto del tráfico como por ejemplo los paquetes que tienen destino Internet tomen la ruta de back-up logrando así la distribución del tráfico por los dos canales.

Si alguna de la dos rutas no está operativa tanto el route map como la tabla de enrutamiento enviarán el tráfico solo por la ruta operativa logrando un respaldo mutuo entre el canal principal y el canal de back-up.

10.2 PRUEBAS

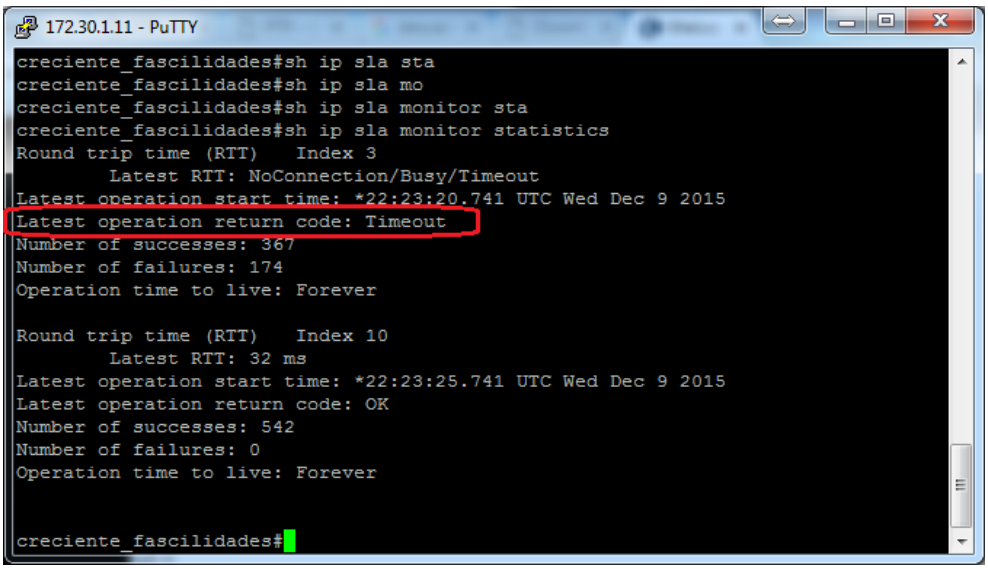
Para verificar el correcto funcionamiento de la configuración de los router se realizaron tres pruebas para confirmar que el canal de back-up y principal siempre estuvieran activos y que uno fuera respaldo del otro en caso de falla. En la primer prueba se simula la falla del canal principal para confirmar que todo el tráfico se redireccione al canal de back-up, en la segunda prueba se

simula la caída del canal de back-up para confirmar que todos los paquetes tomen la ruta principal, y por último se dejan los dos canales operativos para confirmar la distribución del tráfico dependiendo del criterio de selección del cliente. Para todas estas pruebas se toma como referencia la topología de red de la sede La Creciente … Véase el numeral 7.1 …

10.2.1 Pruebas de funcionamiento con el canal principal caído. Para esta prueba se simula una falla del canal principal deshabilitando una de las interfaces del router que conecta con el ISP1 en la ciudad de Corozal, se realizan pruebas para confirmar su caída y observar los cambios en el enrutamiento del servicio. El resultado de estas pruebas se evidencia en las figuras 32 y 33.

Se confirma en las estadísticas de los SLAs del router de La Creciente que el SLA con índex tres el cual monitorea la ruta principal no responde dando como resultado un timeout, además se observa el SLA con índex 10 que monitorea la ruta de back-up está operativo dando como resultado OK.

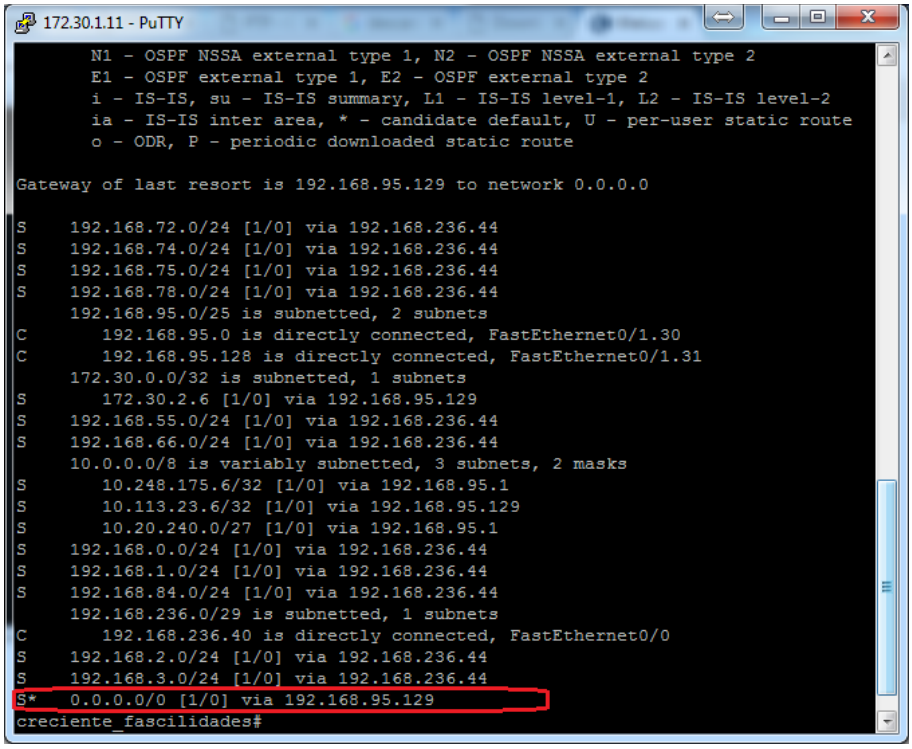
Figura 32. Consulta IP SLA canal principal caído



Fuente. El autor

Se verifica la tabla de enrutamiento del router de La Creciente y se observa que la ruta por defecto o Gateway de último recurso apunta hacia el canal de back-up con la IP 192.168.95.129. El Gateway de último recurso es utilizado por el router para encaminar los paquetes que no tienen una ruta específica dentro de la tabla de enrutamiento como por ejemplo los paquetes que tienen como destino internet, ver figura 33.

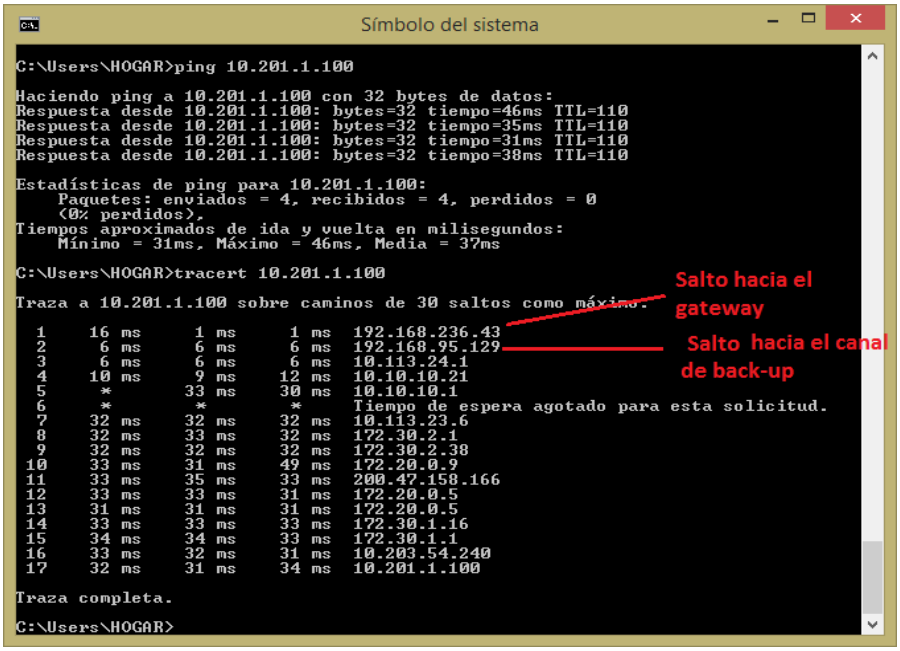
Figura 33. Tabla de enrutamiento canal principal caído



Fuente. El autor

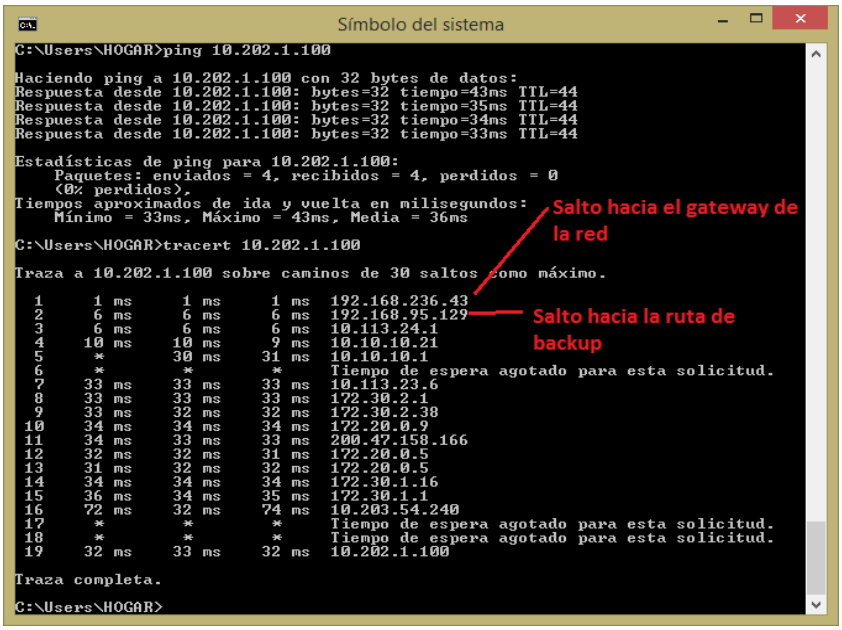
Se realizan pruebas de ping y trazas para determinar que camino toman los paquetes que se dirigen hacia las redes de servidores y los que tienen un destino diferente de esas redes como por ejemplo los paquetes que van hacia Internet. El resultado de estas pruebas se muestran en las figura 34 a la 40.

Figura 34. Pruebas ping y traza canal principal caído



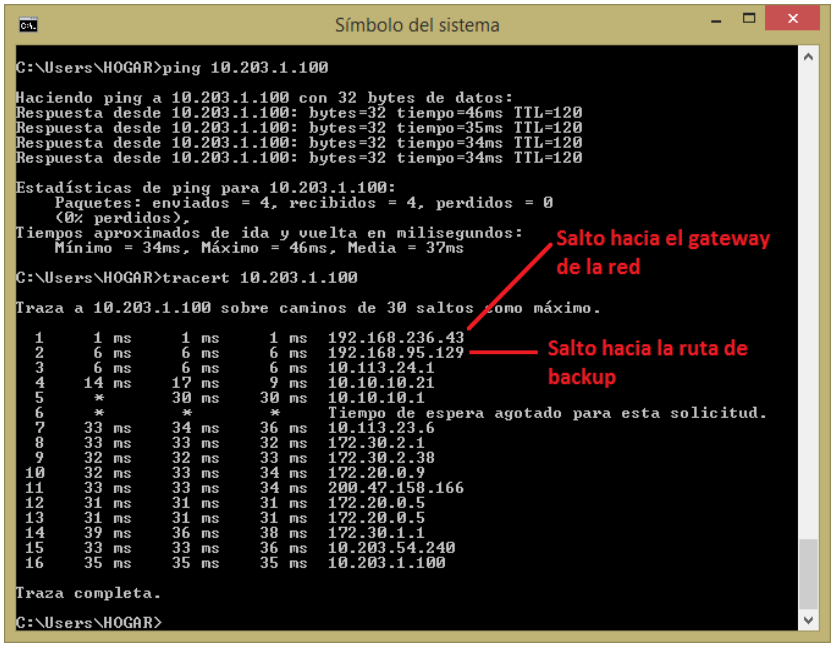
Fuente. El autor

Figura 35. Pruebas ping y traza canal principal caído 2



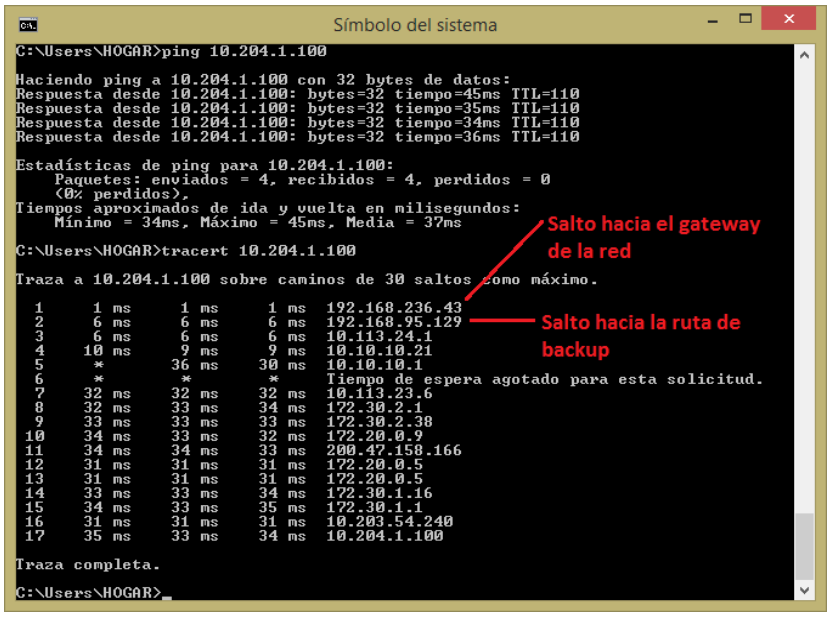
Fuente. El autor

Figura 36. Pruebas ping y traza principal caído 3



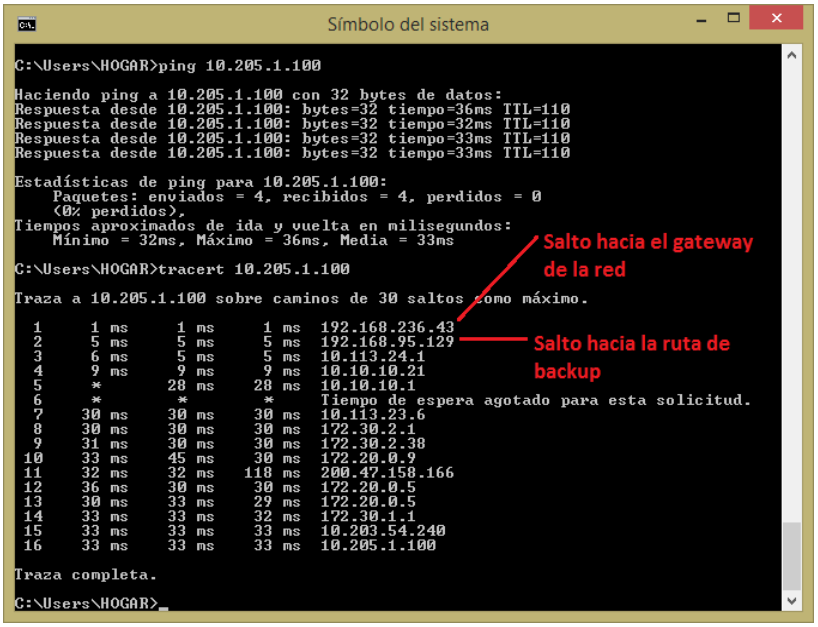
Fuente. El autor

Figura 37. Pruebas ping y traza principal caído 4



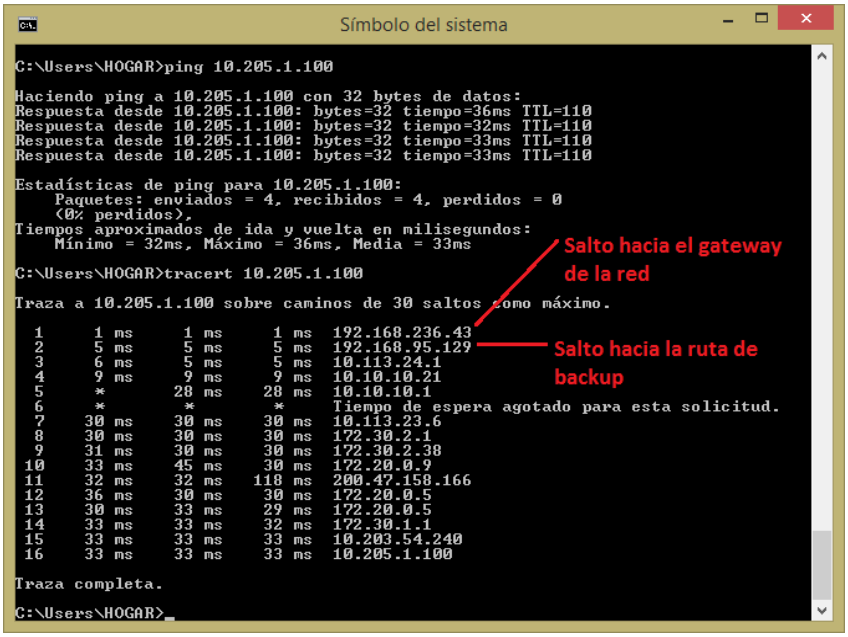
Fuente. El autor

Figura 38. Pruebas ping y traza principal caído 5



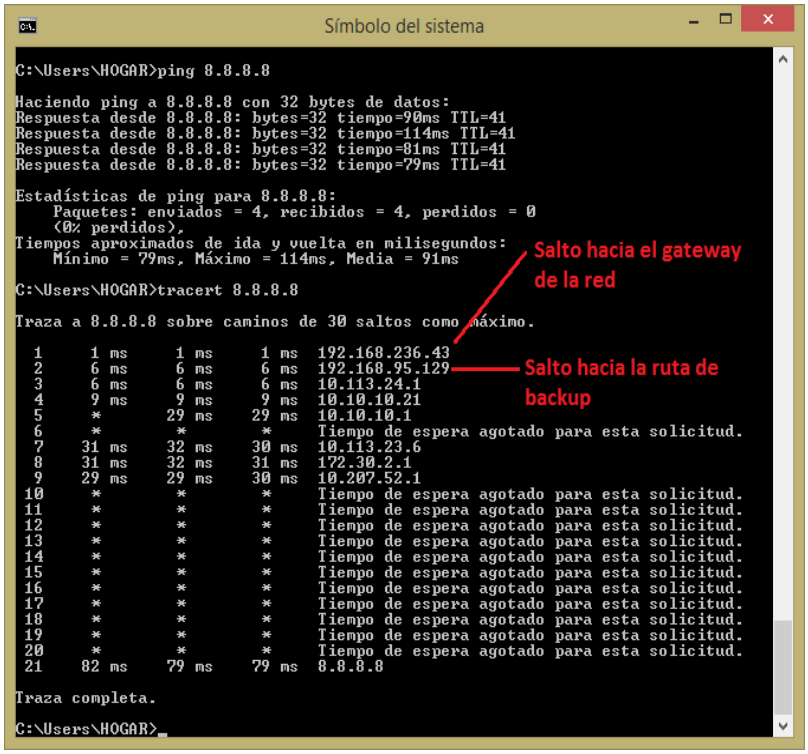
Fuente. El autor

Figura 39. Pruebas ping y traza principal caído 6



Fuente. El autor

Figura 40. Pruebas ping y traza principal caído 7



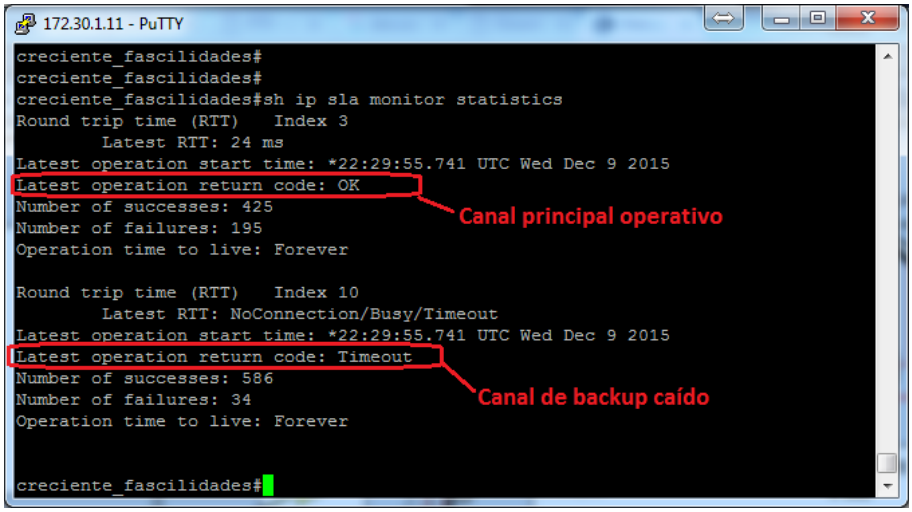
Fuente. El autor

Tomando como referencia la topología de red de La Creciente en la figura 9 … Véase numeral 7.1 … se conecta un PC a la interfaz LAN del router de La Creciente y desde ahí se realizan pruebas hacia los servidores del cliente en Bogotá y hacia una IP publica para confirmar la salida del servicio de Internet. En las pruebas de las figuras 34 a la 40 se muestra que siempre el primer salto en la traza es la IP 192.168.236.43 la cual es la IP de la interfaz LAN del router, el segundo salto en la traza corresponde al router de Corozal por el canal de back-up con la IP 192.168.95.129.

Con estas pruebas se confirma que cuando el canal principal esta caído todo el tráfico toma la ruta de back-up evitando tener problemas de indisponibilidad por la falla de la ruta principal.

10.2.2 Pruebas de funcionamiento con el canal de back-up caído. Para esta prueba se simula la caída del canal de back-up deshabilitando la interfaz del router de Corozal por la ruta de back-up con IP 192.168.95.129, se verifica con las estadísticas de los SLA en el router de La Creciente que el canal principal este operativo y el canal de back-up caído, ver figura 41.

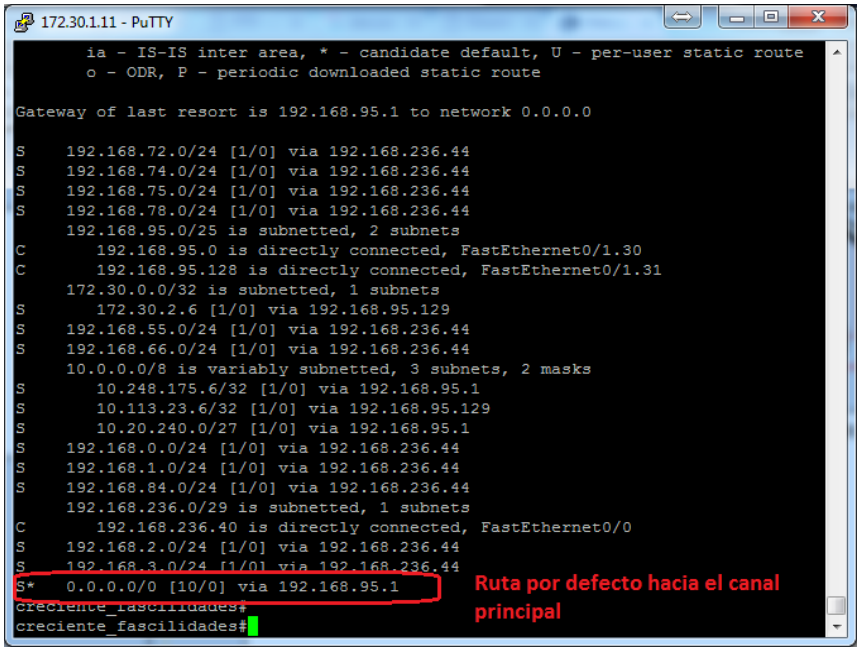
Figura 41. Consulta IP SLA canal back-up caído



Fuente. El autor

Se consulta la tabla de enrutamiento del router de La Creciente para verificar que la ruta por defecto tenga como siguiente salto el canal principal con la IP 192.168.95.1, el resultado de esta consulta se muestra en la figura 42.

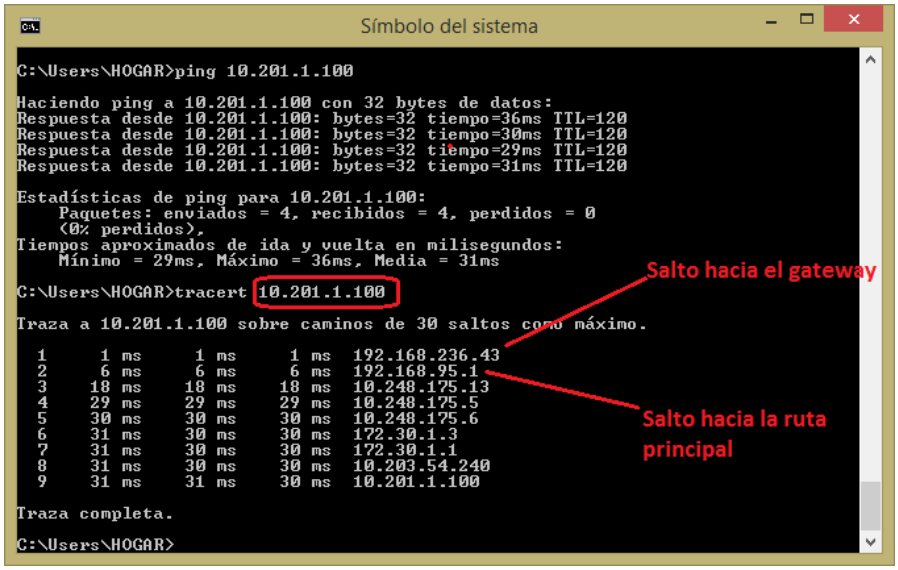
Figura 42. Tabla enrutamiento canal back-up caído



Fuente. El autor

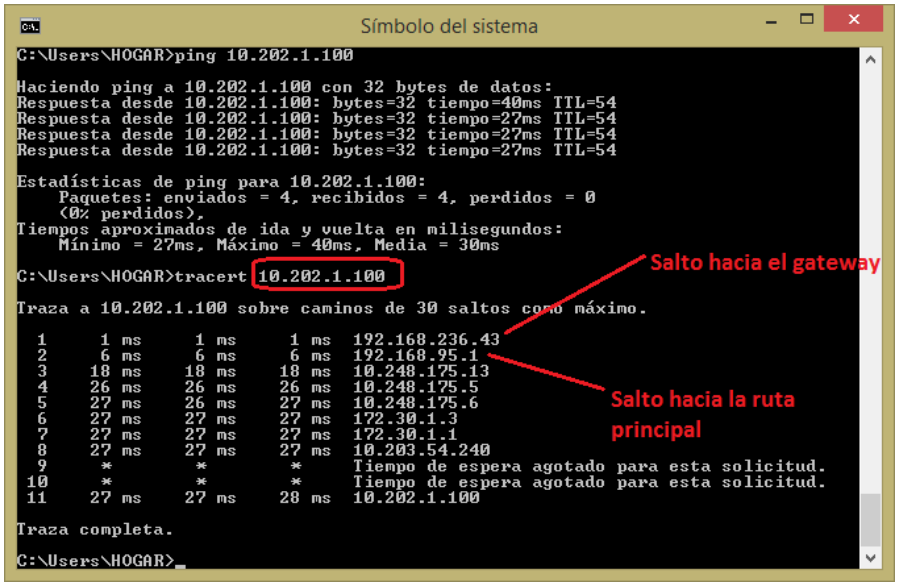
Desde un computador conectado al router de La Creciente se realizan pruebas de ping y trazas para confirma que todos los paquetes tomen la ruta del canal principal para alcanzar las redes de servidores en Bogotá y el servicio de Internet. El resultado de estas pruebas se muestran en las figura 43 a la 48.

Figura 43. Prueba ping y traza canal back-up caído



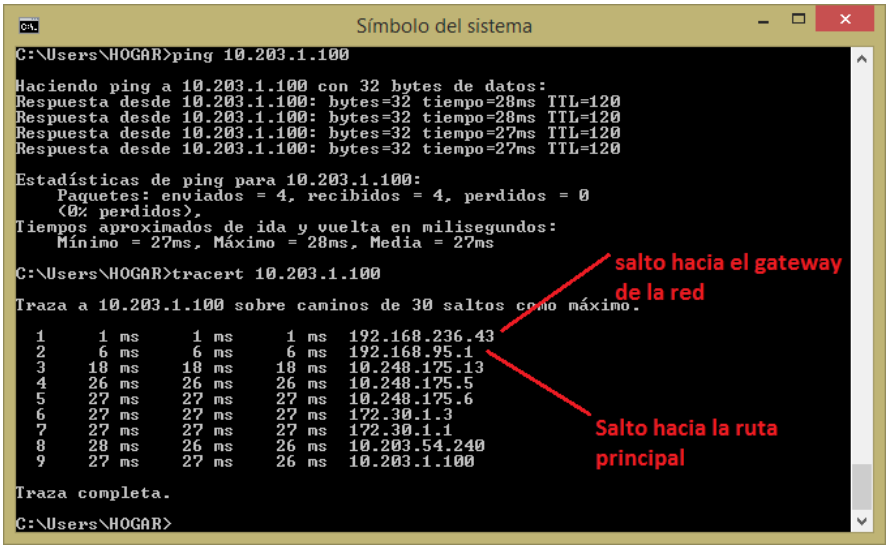
Fuente. El autor

Figura 44. Prueba ping y traza canal back-up caído 2



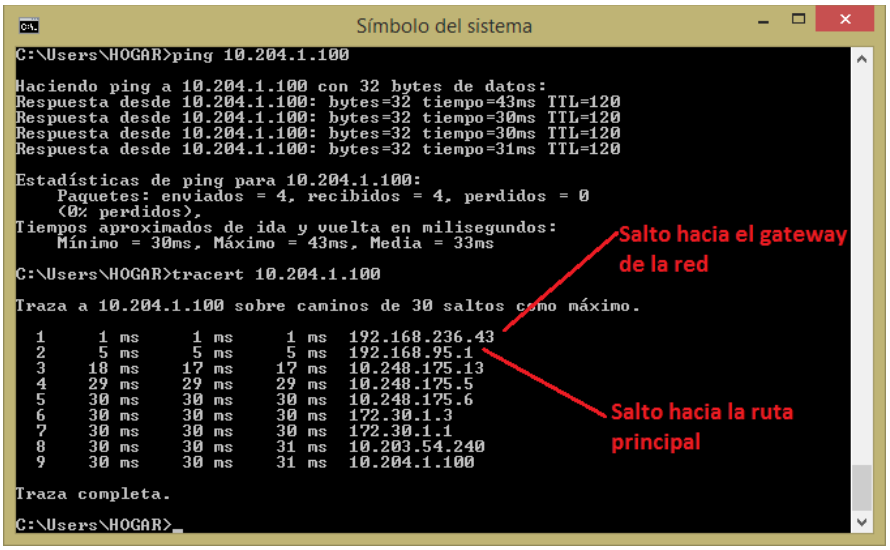
Fuente. El autor

Figura 45. Prueba ping y traza canal back-up caído 3



Fuente. El autor

Figura 46. Prueba ping y traza canal back-up caído 4



Fuente. El autor

Figura 47. Prueba ping y traza canal back-up caído 5

Fuente. El autor

Figura 48. Prueba ping y traza canal back-up caído 6

Fuente. El autor

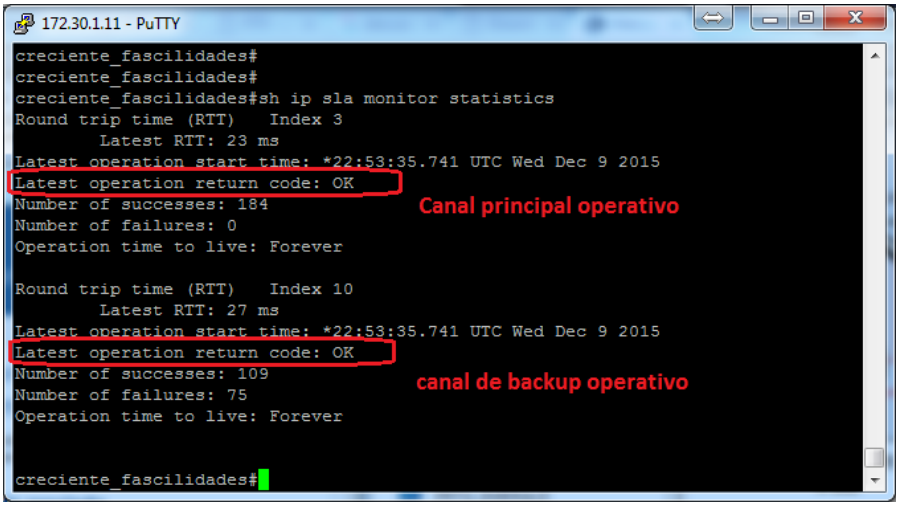
En cada una de las figuras anteriores se evidencia que se realiza una prueba de ping y luego una traza para determinar que ruta toman los paquetes con destino a los servidores 10.201.1.0, 10.202.1.0, 10.203.1.0, 10.204.1.0, 10.205.1.0 y a la IP 8.8.8.8 para probar el servicio de Internet. En todas las trazas se observa que los paquetes tienen como segundo salto la IP 192.168.95.1 que pertenece al router de Enercom en Corozal correspondiente a la ruta principal.

Con estas pruebas se confirma que en el momento que falla el canal de back-up todo el tráfico se envía a través de la ruta principal demostrando que ambos canales se respaldan mutuamente para evitar indisponibilidad en el servicio.

10.2.3 Pruebas de funcionamiento con el canal principal y back-up operativos. Para esta prueba se pretende demostrar que cuando los dos canales están operativos el tráfico se distribuye entre las dos rutas dependiendo del criterio de selección del cliente para aprovechar el ancho de banda de los dos canales y así mejorar el servicio a los usuarios finales.

En esta prueba se debe confirmar a través de las estadísticas de los SLA del router de La Creciente que los dos canales estén operativos, el índex 3 monitorea el canal principal y el índex 10 monitorea el canal de back-up, el resultado de esta consulta se muestra en la figura 49.

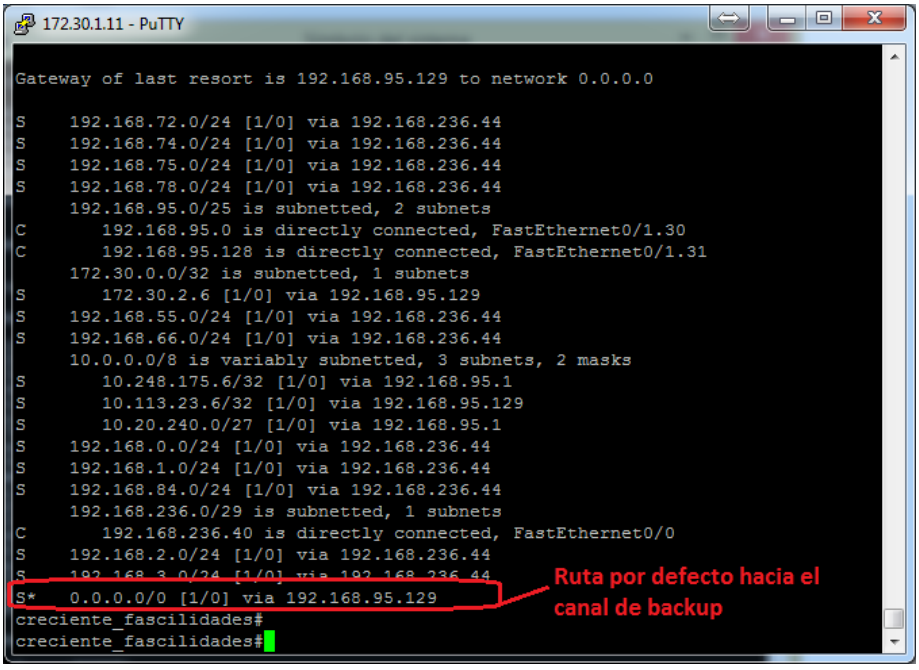
Figura 49. Consulta IP SLA canal principal y back-up activos



Fuente. El autor

Se realiza verificación de la ruta por defecto que se cargó en la tabla de enrutamiento del router de La Creciente, se ejecuta el comando “show ip route” y se observa que la ruta por defecto o gateway de último recurso es la IP 192.168.95.129 correspondiente al canal de back-up, ver figura 50.

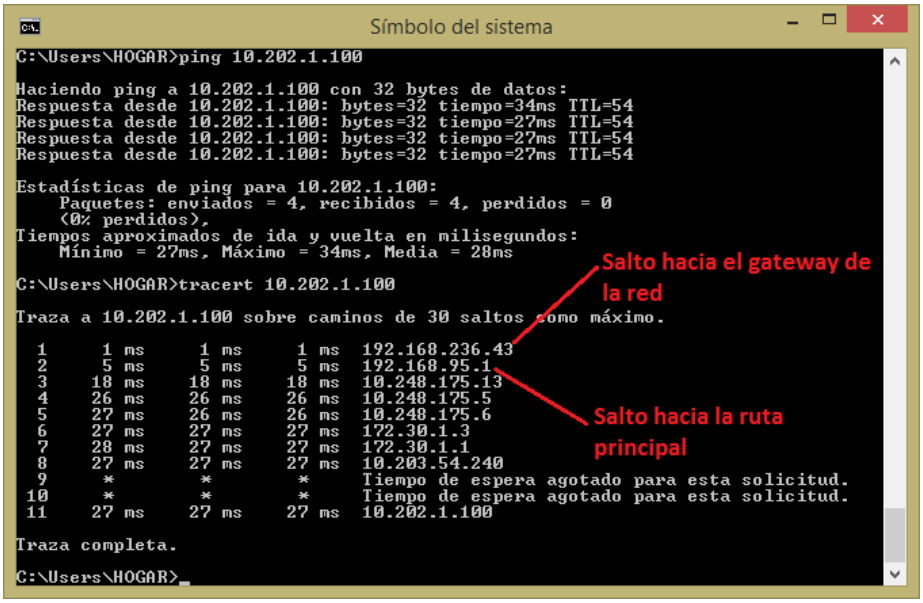
Figura 50. Tabla enrutamiento canal principal y back-up activos



Fuente. El autor

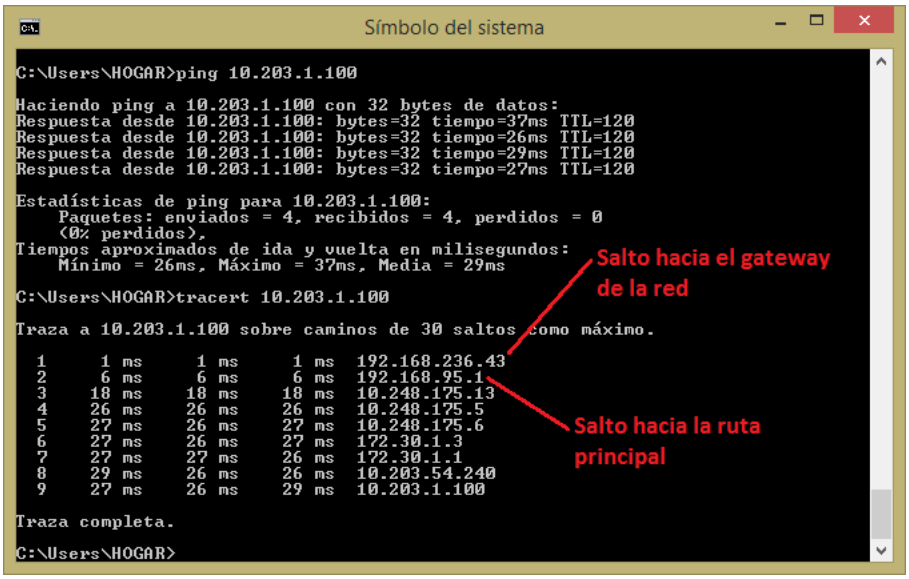
Para confirmar la distribución del tráfico según el criterio de selección del cliente desde un computador conectado al router de La Creciente se realizan pruebas ping y trazas para determinar la ruta que toman los paquetes. En las figura 51 a la 57 se observa el resultado de las pruebas hacia la red de servidores del cliente y hacia Internet para comprobar la distribución del tráfico.

Figura 51. Prueba ping y traza canal principal y back-up activos



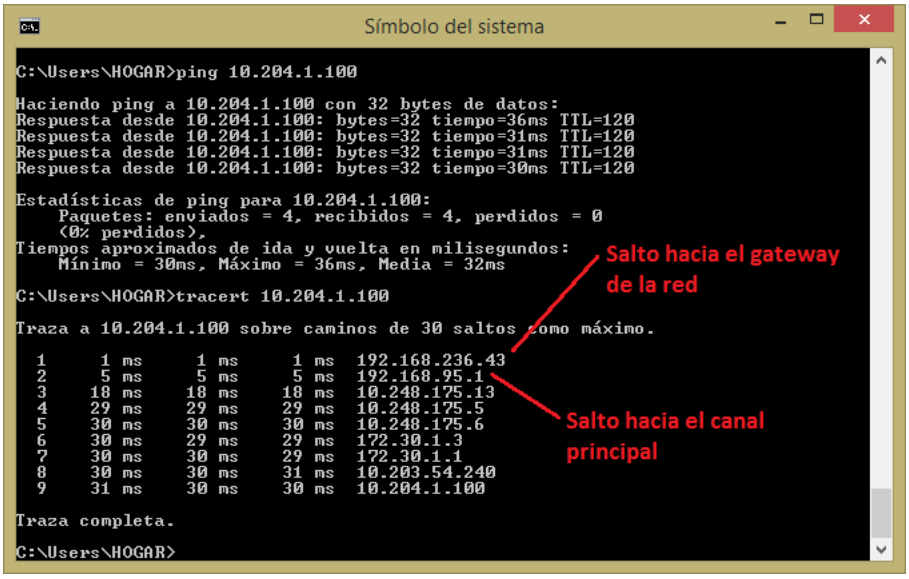
Fuente. El autor

Figura 52. Prueba ping y traza canal principal y back-up activos 2



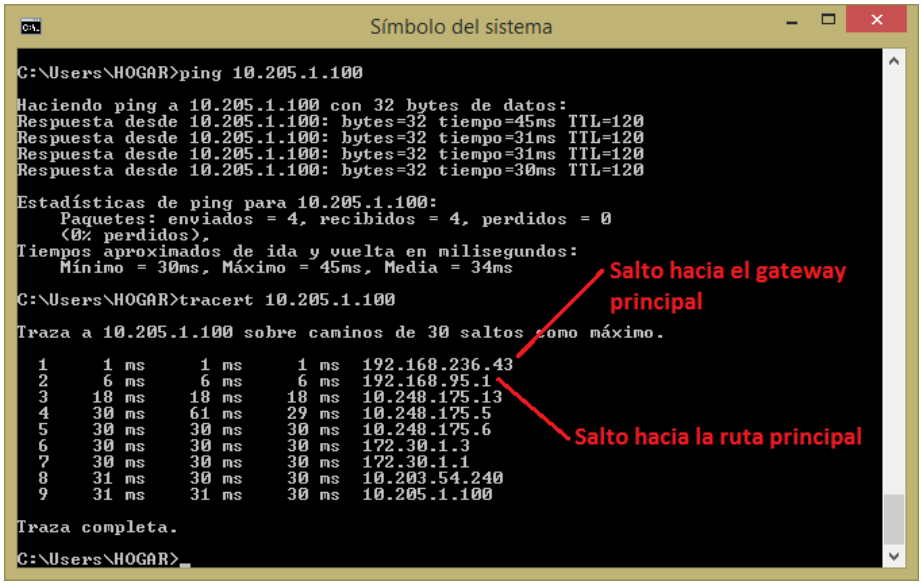
Fuente. El autor

Figura 53. Prueba ping y traza canal principal y back-up activos 3



Fuente. El autor

Figura 54. Prueba ping y traza canal principal y back-up activos 4

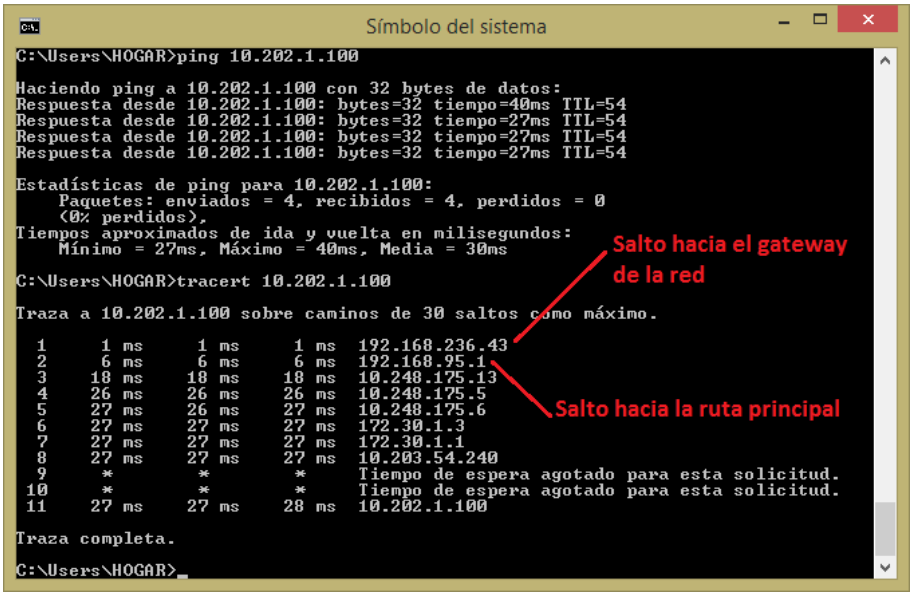


Fuente. El autor

Figura 55. Prueba ping y traza canal principal y back-up activos 5

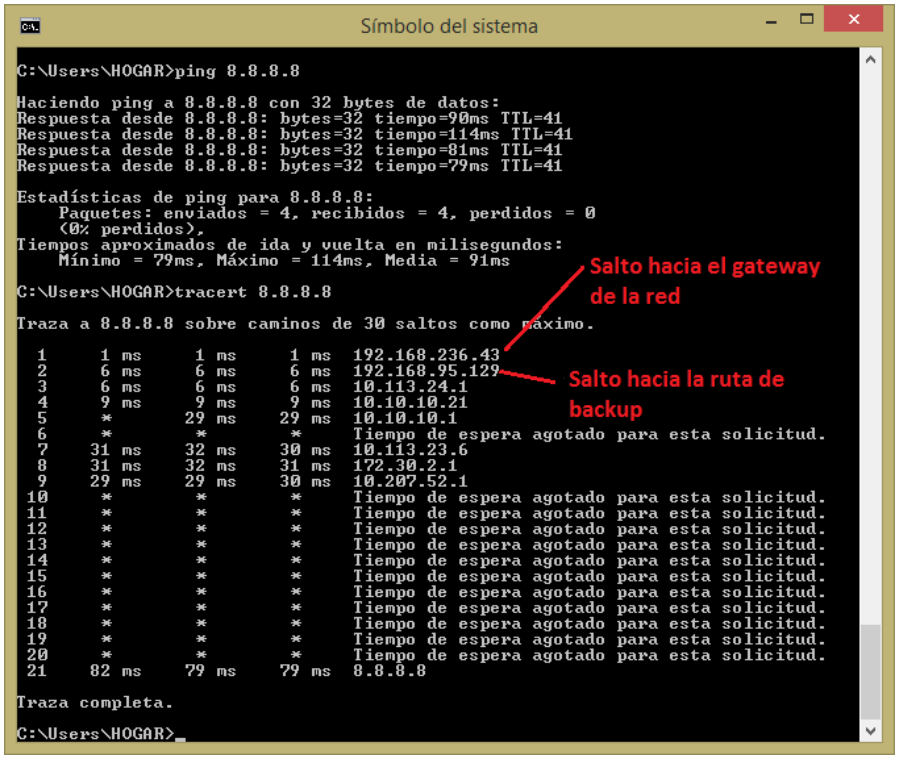
Fuente. El autor

Figura 56. Prueba ping y traza canal principal y back-up activos 6



Fuente. El autor

Figura 57. Prueba ping y traza canal principal y back-up activos 7



Fuente. El autor

Con estas pruebas se evidencia que todos los paquetes que tienen como destino las redes de servidores 10.201.1.0, 10.202.1.0, 10.203.1.0, 10.204.1.0, 10.205.1.0 toman la ruta principal, en las figuras 51 a la 56 se observa inicialmente una prueba de ping hacia una IP valida de la red de servidores y posteriormente una traza la cual muestra que el primer salto hacia su destino es el router de La Creciente con la IP 192.168.236.43, el segundo salto es la IP 192.168.95.1 que corresponde al router de Enercom en Corozal por la ruta principal …véase el numeral 7.1 …. Con esto se da cumplimiento a la primera solicitud del cliente, todo el tráfico hacia los servidores de aplicativos debe tomar la ruta con mayor disponibilidad que en este caso es la ruta principal. En la figura 57 se observa el resultado de la prueba hacia una IP pública para simular el tráfico que tiene como destino Internet, en esta se observa inicialmente una prueba de ping para confirmar conectividad hacia el destino, luego se observa una traza donde el primer salto es nuevamente el router de la sede La Creciente con IP 192.168.236.43, el segundo salto es el router de Corozal con

la IP 192.168.95.129 correspondiente a la ruta de back-up. Con esta última prueba se confirma que todo el tráfico que no es relevante para el cliente como lo es el servicio de Internet se envía por la ruta de back-up que es la ruta menos confiable.

Con las pruebas realizadas se confirma que la configuración aplicada al router de La Creciente permite una distribución de tráfico cuando el canal principal y back-up están operativos, además se confirma que los dos canales se respaldan mutuamente en caso de falla para evitar indisponibilidad del servicio.

11. CONCLUSIONES

Con el desarrollo de este proyecto se logra llegar a una configuración para los enrutadores de la sede de La Creciente que permite utilizar los dos canales, principal y back-up, para enviar y recibir tráfico simultáneamente de la red del cliente, se comprueba que utilizando la técnica de enrutamiento PBR (Policy Base Routing) y las ACL (Access Control List) se logra que el cliente seleccione como distribuir su tráfico dependiendo de su relevancia distribuyendo la ocupación del canal lo que ocasiona que se aumente el ancho de banda para tener una mayor fluidez y velocidad en los aplicativos y servicios que utilizan los usuarios finales, a su vez, se confirma que utilizando las herramientas IP SLA y Track incluidas en el IOS de los enrutadores Cisco se genera un monitoreo y respaldo mutuo entre los dos canales disminuyendo la indisponibilidad del servicio en caso de fallas.

Para el cliente fue muy importante que se lograra distribuir el tráfico entre los canales principal y back-up ya que luego de las pruebas realizadas y el efecto positivo en el desempeño de la red solicitaron que se implementara en todos los canales similares a los de la sede de La Creciente, además se creó la percepción que los recursos y dineros que se invierten en los canales de respaldo o back-ups son mejor aprovechados si se implementa esta configuración que permite utilizar los dos canales en todo momento sin perder la esencia del respaldo de un canal de back-up. Luego de la implementación de esta configuración en la sede de La Creciente se sostuvieron conversaciones informales con algunos usuarios finales en donde manifestaron que luego de los cambios realizados en la red sus aplicativos funcionaban mejor, tenían una respuesta más rápida ayudando a agilizar sus procesos y labores diarias.

Para Enercom S.A es un logro positivo cumplir con las exigencias y expectativas de sus clientes y a su vez este tipo de configuraciones se convierten en un valor agregado a los servicios y productos que se ofrecen en el mercado logrando diferenciarse de la competencia y aumentan la confianza

de los clientes como una empresa capaz de cumplir con las nuevas exigencias y dinamismo del mercado.

12. BIBLIOGRAFÍA

ARIGANELLO, Ernesto. Enrutamiento IP. En. Redes Cisco: Guía de Estudio para la Certificación CCNA 640-802. México: Alfaomega, 2009. P. 57 -59.

ARIGANELLO, Ernesto y BARRIENTOS SEVILLA, Enrique. Implementaciones con cisco IOS. En. Redes Cisco CCNP a fondo Guía de estudios para profesionales. México: Alfaomega, 2010. P. 188-191.

BATEMAN, Andy. Comunicaciones digitales diseño para el mundo real. España. Marcambo S.A. 2003. 223p

Cisco System. Access control list: overview and guidelines [en línea]. Version 12.2. San José (California). Cisco System. [Citado en 2015-03-15]. Disponible en: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfacls.html#wp1000893

Cisco System. Configuring IP SLA [en línea]. Versión 12.4. San José (California). Cisco System. [citado en 2015-03-15]. Disponible en: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/44sg/configuration/guide/Wrapper-44SG/swipsla.html

Cisco System. Configuración de listas de acceso IP [en línea]. San José (California). Cisco System. [citado 2015-03-15]. Disponible en: http://www.cisco.com/cisco/web/support/LA/7/75/75923_confaccesslists.pdf

Cisco System. Software de red (IOS y NX-OS) [en línea]. San José (California). Cisco System. [citado en 2016-02-28]. Disponible en: http://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-software-releases-listing.html

ENERCOM S.A. Organigrama [en línea]. Versión 3. Enercom [citado en 2015-07-17]. Disponible en: http://192.168.15.12:8081/alfresco/d/d/workspace/SpacesStore/34fa00d9-4285-4f01-bed7-aa042b462a72/organigrama.pptx

ENERCOM S.A. LA CRECIENTE PRINCIPAL [programa de computador en disco]. Enercom [citado en 2015-05-04]. Disponible en: http://192.168.15.4:81/group.htm?id=0&tabid=1

ENERCOM S.A. LA CRECIENTE BACKUP [programa de computador en disco]. Enercom [citado en 2015-05-04]. Disponible en: http://192.168.15.4:81/group.htm?id=0&tabid=1

FREEDMAN, Alan. Glosario de computación. México. McGraw-Hill. 1984. 396 p.

HEWLETT-PACKARD . Policy based routing. Texas. Hewlett-packard [citado en 2015-03-15]. Disponible en: https://www.google.com/patents/US20140029619

ROMERO TERNERO, María del Carmen, *et ali*. Redes locales. ed. 2ª. España. Parainfo S.A. 2014. 294 p.